Otros títulos publicados por Ediciones Vía Libre:

Prohibido Pensar, Propiedad Privada
[2006]

Monopolios artificiales sobre bienes intangibles
[2007]

Libres de monopolios sobre el conocimiento y la vida. Hacia una convergencia de movimientos
[2008]

Versiones electrónicas para descarga en **http://www.vialibre.org.ar/materiales**

"Ustedes ni nosotros jamás conseguiremos afirmar con esta tecnología que la inviolabilidad del secreto del voto de cada ciudadano está a resguardo de su derecho supremo, sino que únicamente conseguiremos confiar en que las personas a cargo de estas tecnologías hacen lo correcto. [...] Hoy con más experiencia y responsabilidad que la que tuvimos cuando asumimos la tarea de instrumentar la modalidad del voto electrónico, estamos convencidos que no volveríamos a repetir el modo."

(Fragmentos del Informe de la Junta Electoral de San Antonio Oeste presentado ante el Consejo Deliberante tras las pruebas de voto electrónico realizadas el 16 de diciembre de 2007. Las Grutas, Río Negro, Argentina)

Los avances de las nuevas tecnologías de la información y comunicación (TICs) tienen un correlato que se traduce en una forma de romanticismo tecnológico, una ideología fundada en la creencia de que el halo de la informática otorga transparencia, rapidez, reducción de costos. Esta ideología técnica aplicada al proceso electoral pone en riesgo los valores fundantes de la democracia: el secreto y la universalidad del voto y el derecho ciudadano a participar del control del proceso electoral mismo. El voto electrónico es quizás el emergente más claro de esa ideología que plantea que agregar la letra e- adelante de la palabra Gobierno nos dará mejor gobierno, mejor educación o mejores empleos.

La "fe en la Secta de San Byte", como la llama Pedro Rezende en esta misma publicación, nos puede llevar a un callejón sin salida cuando se trata de incorporar tecnologías en el proceso electoral sin la debida evaluación de problemas, costos sociales y violación de principios básicos para nuestra ciudadania.No existe tecnología para resolver problemas políticos, sin embargo, estos sistemas se siguen difundiendo bajo la creencia de que mejorarán la democracia y la transparencia del proceso electoral. Poco se discute al respecto y se escuchan muy pocas voces independientes en la materia. Esta publicación pretende ser un llamado al debate y un insumo de información para enriquecer la discusión que necesariamente tenemos que dar frente a la aparentemente consensuada voluntad política de informatizar el acto mismo de votar.

http://www.votoelectronico.org.ar

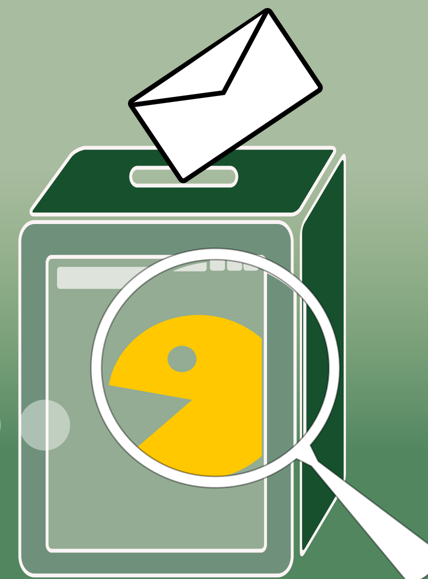


ISBN 978-987-22486-5-9



Voto Electrónico Los riesgos de una ilusión

Voto electrónico
Los riesgos de una ilusión



Ediciones Vía Libre

FUNDACIÓN HEINRICH BÖLL



Fundación Vía Libre

Fundación Vía Libre es una organización sin fines de lucro radicada en Córdoba, Argentina. Desde el año 2000 trabaja en difusión del conocimiento y desarrollo sustentable, partiendo de los postulados del movimiento global de Software Libre. Vía Libre trabaja en defensa de la libertad y los derechos ciudadanos en el marco de la inclusión de nuevas tecnologías de información y comunicación en nuestra vida ciudadana. En ese marco, mantiene el sitio http://www.votoelectronico.org.ar como forma de alertar a la ciudadanía sobre los riesgos de la incorporación de nuevas tecnologías en el acto de emisión del sufragio.

http://www.vialibre.org.ar

Fundación Heinrich Böll

La Fundación Heinrich Böll es una fundación política alemana sin ánimo de lucro, cercana al partido de la Alianza 90/Los verdes.
Con el fin de incentivar la promoción de ideas democráticas, la participación ciudadana y el entendimiento internacional, su trabajo se centra en fomentar los valores políticos de la ecología y el desarrollo sustentable, los derechos de la mujer y la democracia de género, la democracia y la ciudadanía, diversidad de medios y la formación de una opinión pública crítica. Además, la Fundación Böll promueve el arte, la cultura, la ciencia, la investigación y el desarrollo internacional.

http://www.boell-latinoamerica.org/

Voto electrónico

Los riesgos de una ilusión





FUNDACIÓN HEINRICH BÖLL

VOTO ELECTRÓNICO: LOS RIESGOS DE UNA ILUSIÓN

Beatriz Busaniche; Federico Heinz; Alfredo Rezinovsky [et alt.]
1ra ed. Córdoba: Fundación Vía Libre, 2008. 140 p. ; 21x15 cm.

ISBN 978-987-22486-5-9

Edición a cargo de Beatriz Busaniche y Federico Heinz

Correcciones: Oscar Heinz, Rayentray Tappa y Octavio Sebastián
Diseño editorial: Proyecto nómade [www.nomade.org.ar]. Tapa e ilustraciones: Luis Britos. Diseño de página: Lila Pagola. El diseño está realizado con software libre y licenciado bajo Creative commons by-sa Argentina 2.5

Voto electrónico

Los riesgos de una ilusión

Indice

Anexo

SOBRE LAS ORGANIZACIONES PARTICIPANTES

Fundación Vía Libre

Fundación Vía Libre es una organización sin fines de lucro radicada en Córdoba, Argentina. Desde el año 2000 trabaja en la difusión del conocimiento y desarrollo sustentable, partiendo de los postulados del movimiento global de Software Libre. Vía Libre trabaja en defensa de la libertad y los derechos ciudadanos en el marco de la inclusión de nuevas tecnologías de información y comunicación en nuestra vida ciudadana. En ese marco, mantiene el sitio http://www.votoelectronico.org.ar como forma de alertar a la ciudadanía sobre los riesgos de la incorporación de nuevas tecnologías en el acto de emisión del sufragio.

http://www.vialibre.org.ar

Fundación Heinrich Böll

La Fundación Heinrich Böll es una fundación política alemana sin ánimo de lucro, cercana al partido de la Alianza 90/Los verdes. Con el fin de incentivar la promoción de ideas democráticas, la participación ciudadana y el entendimiento internacional, su trabajo se centra en fomentar los valores políticos de la ecología y el desarrollo sustentable, los derechos de la mujer y la democracia de género, la democracia y la ciudadanía, diversidad de medios y la formación de una opinión pública crítica. Además, la Fundación Böll promueve el arte, la cultura, la ciencia, la investigación y el desarrollo internacional.

http://www.boell-latinoamerica.org

Prefacio

Richard M. Stallman

Votar con computadoras es abrir una puerta grande al fraude. La computadora ejecuta un programa, y el programa puede ser cambiado o reemplazado. Puede ser reemplazado temporalmente durante la elección por otro diseñado para dar totales falsos. Ningún estudio del programa que debería correr puede asegurar que otro programa no actúe mal.

La votación es una actividad especial porque normalmente el votante no puede averiguar, según los totales, que su voto ha sido contado correctamente, y hay que desconfiar de todas las partes involucradas.

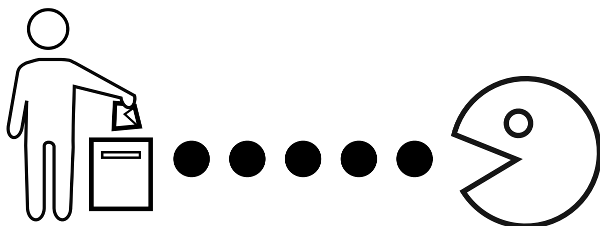
No podemos dar por supuesto que el fabricante es honesto, ni que la autoridad electoral es honesta, ni que los dos no conspiran juntos.

El sistema electoral debe ser a prueba de todas las posibilidades, pero ésto es imposible con una computadora.

Muchos activistas de software libre piensan que usar el software libre en la máquina de votación asegura una elección honesta. Usar software privativo es malo aquí, como siempre: el fabricante podría diseñarlo a sus anchas para fraude. Pero ser libre no basta, porque luego la autoridad electoral podría hacer el fraude. El único sistema confiable es votar con papel.

Algunos investigadores han propuesto sistemas muy sutiles de encriptación para votar. Dicen que con esos sistemas el fraude es imposible. Quizás tengan razón, pero tal conclusión no es fácil de comprobar con certeza. Si algún día parece haber un sistema de confianza para el voto digital, la sociedad debe probarlo gradualmente, a lo largo de una década. En los sistemas electorales, cambiar con prisa es arriesgar todo.

Primeros pasos



Introducción

Vivimos en tiempos de revolución tecnológica.

Por encima de cualquier apreciación sobre el tema, los avances en lo que se refiere a Tecnologías de Información y Comunicación (TICs) de los últimos 50 años son asombrosos. Hemos acortado distancias, aumentado exponencialmente nuestra capacidad de procesar información, potenciado nuestro poder de cálculo, maximizado la productividad y construido dispositivos y teorías que nos permiten manipular la información que constituye la naturaleza misma. A la vez, hemos desarrollado un bagaje ideológico que acompaña esta revolución científico-técnica que algunos pensadores denominan "sociedad de la información" o "sociedad del conocimiento".

Actualmente, la ideología técnica viene a cubrir aquello que siglos atrás cubría la religión, luego la política, y finalmente la ciencia: explicar y normar el mundo. Las tecnologías se presentan hoy como la encarnación de los valores de una sociedad democrática: la libertad, la igualdad y el intercambio. "Estamos aquí en el corazón de la ideología técnica, en esa tentación de investir a una herramienta de la capacidad para resolver un problema social, cultural y político relevante con otra lógica. Su fuerza como ideología es triple. Descalificar cualquier discurso que se atreva a poner en cuestión el vínculo entre el rendimiento de las herramientas y los problemas de la sociedad. Ser transnacional e influir en la juventud. Mantener un bajo perfil no presentándose bajo la forma de un discurso construido y coherente,[...] Es una forma de la sensatez, que explica la dificultad de la crítica, porque la ideología nunca resulta tan fuerte como cuando es trivial y cotidiana".[1]

Esta lúcida descripción del catedrático francés Dominique Wolton nos sirve para ingresar de manera crítica a uno de los emergentes más claros de la ideología técnica hoy día: el voto electrónico. Es en este supuesto avance de la técnica donde se cristaliza de manera más elocuente esa ideología que pretende otorgar a las herramientas de la informática el poder de mejorar los problemas sociales. Se lo presenta como un sistema que nos ayudará a mejorar la democracia, partiendo del desmantelamiento del aparato partidario y el punterismo, hasta el fomento de la participación ciudadana, como si la inclusión de tecnologías en el acto de votar lo revistiera de transparencia, celeridad y, por sobre todo, modernidad.

Oponer una voz de alerta a una 'obvia' innovación como ésta convierte a quienes lo hacemos en ludditas en potencia, en interesados en conservar lo viejo (y por tanto, todo lo malo) de la política. Es en este tema donde la ideología técnica opera con una soltura y una trivialidad asombrosa: ¿Quién se atrevería a negar lo 'obvio'? ¿Quién podría negarse a modernizar un acto central de nuestras democracias? ¿Quién podría negarse a pensar que en aquellos ámbitos donde la información se procesa mediante tecnologías reina la neutralidad y la transparencia?

Ciertamente, quienes venimos del campo de la política de la tecnología, como los activistas del software libre, sabemos perfectamente que las tecnologías distan mucho de ser neutrales y que existen discusiones sobre quién controla realmente los avances de la ciencia y la técnica. Quizás esa sea la razón por la cual el voto electrónico, que tanto y tan profundamente ha permeado en grandes sectores no lo ha hecho entre quienes trabajan en Software Libre o se especializan en seguridad de sistemas de información, ámbitos en los que genera desconfianzas profundas.

Será tal vez porque desde esos sectores que trabajan cotidianamente con las nuevas tecnologías se entiende realmente que la idea de neutralidad y transparencia asociada a la tecnología no es más que una falacia y una construcción que se ha impuesto a fuerza de discursos interesados, armados para consolidar estas herramientas. Misteriosamente, o tal vez no, son estos sectores los que están deliberadamente excluidos del debate sobre voto electrónico.

Alfredo Rezinovsky, uno de los autores de este libro, llama la atención permanentemente sobre la forma en la que se discuten las tecnologías electorales: por un lado se presentan los políticos, los sociólogos y politólogos, expertos en derecho y abogados; sin embargo, a la hora de convocar a los que ofrecen las explicaciones técnicas, los que siempre están presentes son los ingenieros y vendedores de las firmas que distribuyen y comercializan los dispositivos de votación. Rara vez se encuentra en esos

debates a los expertos en seguridad de sistemas de información independientes que presentan más advertencias, alertas y reparos, que romances y utopías.

No deja de sorprender el hecho de que toda vez que elevamos una voz de alerta, se escucha por parte de la ciudadanía una voz de asombro. Por alguna razón, 'la gente' (un colectivo tan heterogéneo que es imposible de definir) cree en el voto electrónico, sin pensar mucho más. Si las tecnologías están en todas partes y eventualmente han mejorado nuestras vidas de alguna manera, entonces deberían servir para mejorar nuestras democracias. Así funciona la trivialidad de esta ideología que ha permeado hasta las escuelas, donde, a decir de Patricio Lorente en su texto, se enseña que el voto electrónico es más transparente y eficiente para emitir el sufragio, sin ofrecer prueba alguna de semejante afirmación.

Probablemente no haya mejor noticia para quienes advertimos sobre estos problemas, que la aparición de Homero Simpson lidiando con una máquina de votación que cambia deliberadamente su voluntad y manipula su voto hasta triturarlo. La imagen de Homero cuestionando el voto electrónico tiene más fuerza pública que los documentos académicos que vienen presentando matemáticos, criptógrafos, expertos en seguridad desde hace más de veinte años. Los centros de estudio de universidades como Princeton y California, o los profesores de informática y computación de las principales universidades de Brasil, entre otros, han dado voces de alerta, presentado documentación consistente y sólida sobre las falencias de seguridad de los sistemas, pero ninguno de ellos tendrá el impacto mediático y social de Homero Simpson en el capítulo donde pretende votar a Obama y su voto va, multiplicado por seis, a John McCain. Así es como funciona la ideología técnica y quizás desde esa misma lógica se la pueda desnudar.

Esta publicación no tiene otro fin que el de abrir un debate imprescindible antes de que sea demasiado tarde. Ilustrar a lectores no avezados en el campo de las tecnologías, sobre cómo funcionan realmente estos sistemas y dar la voz de alerta sobre los riesgos de creer que existen tecnologías que mejoren nuestras democracias así sin más. Nunca las soluciones mágicas han dado buenos resultados y este caso no es la excepción. Como bien dice el legislador Abrevaya en su intervención para el debate, "en la medida en que la comunidad no esté involucrada no va a haber ningún sistema que tenga capacidad de modificar esta realidad". Aún peor, en la medida en que como sociedades tomemos la decisión de tercerizar y privatizar nuestro sistema, y con él nuestra responsabilidad electoral, hasta el acto mismo de emitir el voto, cada vez será más dificil la intervención de la comunidad en un proceso que nos pertenece como ciudadanos, que es de todos y que nos ha costado años de lucha recuperar.

Este libro no sería posible sin el apoyo invalorable de la Fundación Heinrich Böll y en particular de su flamante oficina en Santiago de Chile, desde donde se tomó la decisión de acompañar esta publicación para contribuir a un debate importante sobre las democracias y la participación ciudadana en América Latina.

Agradecemos también a Gabriel Diner, asesor del legislador de la ciudad de Buenos Aires Martín Hourest, quien tuvo la visión de informarse y atender con detalle un tema que está en un punto de discusión álgido en la Ciudad de Buenos Aires, y quien además nos abrió las puertas para llevar esta discusión al corazón mismo de la Legislatura, donde en definitiva se toman las decisiones que nos afectan como ciudadanos.

A Pedro Rezende, profesor de matemática de la Universidad de Brasilia, uno de los catedráticos más destacados en seguridad de sistemas de información, que es a su vez, un incansable luchador por la desmitificación de la 'Secta de San Byte'.

En la localidad de Las Grutas y la provincia de Río Negro, ha sido fundamental el trabajo del periodista Sergio Ploss, quien dio la voz de alerta y movilizó a la ciudadanía cuando se implementó el sistema en diciembre de 2007. Allí, el trabajo de Iván Santander ha dado frutos importantes y lo mismo ha sucedido con la visión de la legisladora María Liliana Gemignani, quien tuvo la grandeza de movilizar una autocrítica rara vez vista por parte de los tomadores de este tipo de decisiones.

En Ushuaia, Roberto Sprenger, Marcelo Papuccio y la Fundación Apertura Digital, acompañaron también estos procesos llamando la atención permanentemente y aportando solidez al debate.

Agradecemos también a los colaboradores y amigos de la Fundación Vía Libre, que nos han ayudado con la corrección y recopilación de materiales para esta publicación. Es difícil nombrar a todos, pero especialmente queremos agradecer a Ariel Wainer, Gabriel Acquistapace, Marcela Tiznado, Román Gelbort, Alfredo Rezinovsky, Oscar Heinz, Enrique Chaparro, Patricio Lorente, Rayentray Tappa, Luciano Rossi, sin cuya ayuda y apoyo, esta publicación no se hubiera terminado jamás a tiempo.

Finalmente, queremos destacar el trabajo de Lila Pagola, Luis Britos y el proyecto Nómade, un colectivo de articulación de artistas que trabajan con Software Libre bajo los postulados del movimiento por la cultura libre. Su trabajo editorial y de diseño integramente realizado con Software Libre son esenciales para que estas discusiones lleguen a más gente y sean más amenos y accesibles para nuestros lectores.

Esperamos que esta publicación y sus presentaciones nos ayuden a comprender que nuestras democracias no se

mejoran con informática, sino con compromiso y participación ciudadana. Eso aspiramos lograr, y a esa misión nos hemos dedicado. Este libro es una herramienta más en ese sentido. Muchas gracias.

Beatriz Busaniche y Federico Heinz
Fundación Vía Libre - Editores

Para más información visite:
http://www.votoelectronico.org.ar/ y
http://www.vialibre.org.ar/

Notas

1- Wolton, Dominique. "Pensar la Comunicación" Editorial de la Universidad Nacional de Tres de Febrero. Prometeo Libros. ISBN 978-987-574-132-4

¿Qué es el voto electrónico?

Beatriz Busaniche y Federico Heinz

Existen varias definiciones para lo que se denomina comúnmente "voto electrónico". En un sentido amplio, se considera voto electrónico a la incorporación de recursos informáticos en cualquier parte del proceso electoral, ya sea en el registro de ciudadanos, la confección de mapas de distrito, la logística electoral, el ejercicio del voto en sí mismo, el escrutinio y la transmisión de resultados. Sin embargo, a los fines de esta publicación, vamos a considerar estrictamente dos de las áreas del sufragio: la emisión del voto en sí misma y el recuento de votos de cada punto de votación.

En un sentido estricto denominaremos aquí "voto electrónico" a los mecanismos diseñados para emitir y contar los sufragios en un único acto, a través de algún sistema informático instalado y en funcionamiento en el lugar mismo donde el elector concurre a expresar su voluntad política.

Entonces, entendemos por voto electrónico a todo sistema informatizado para el acto de emitir y contar los votos en la mesa de votación, donde los y las ciudadanas entran en contacto directo con los dispositivos electrónicos. Consideramos voto electrónico al uso de computadoras, urnas electrónicas o dispositivos similares para la emisión y recuento automatizado del sufragio.

Los mecanismos en los que la computadora no está directamente involucrada en el acto de emisión del voto, así como aquellos que utilizan la informática exclusivamente para la automatización del recuento y la consolidación de resultados quedan así expresamente fuera del foco de esta publicación.

Una categoría particular del voto electrónico es el voto a través de internet (a menudo llamado "voto digital"). En

éste, los ciudadanos ni siquiera acuden al centro electoral (sean escuelas, centros cívicos, oficinas públicas, etc.) para expresar su voluntad a través de uno de los dispositivos ya mencionados, sino que lo hacen a distancia, utilizando su propia computadora o la de algún punto de acceso público para conectarse a través de Internet con un sistema central de registro y tabulación de votos.

No existe una única forma de implementar voto electrónico, más bien podríamos decir que existen tres grandes tipos de sistemas a utilizar, que difieren no sólo en su implementación, sino y fundamentalmente en sus riesgos y beneficios. Los mecanismos más frecuentemente identificados como de voto electrónico se pueden agrupar en tres grandes conjuntos: a) los sistemas de recuento automático de votos mediante reconocimiento óptico de las marcas hechas en la boleta por parte de los ciudadanos, que son sistemas que hacen hincapié en el escrutinio electrónico; b) los sistemas de registro electrónico directo (RED, o DRE por su sigla en inglés) ejemplificados comúnmente con los denominados kioscos de votación o urnas electrónicas; c) los sistemas de votación a distancia a través de internet [1].

Notas

1- Voto Electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales. María Inés Tula (coordinadora). Ariel Ciencia Política - CIPPEC Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento. (2005) ISBN 950-9122-90-4

Sistemas usados

Beatriz Busaniche y Federico Heinz

Sistemas de recuento automático

Los primeros sistemas de esta clase datan del siglo XIX, cuando se comenzaron a implementar en la ciudad de Nueva York mediante tarjetas perforadas. Actualmente, la mayoría de los sistemas de este tipo se basan en el reconocimiento óptico de marcas hechas por el votante sobre la boleta, ya sea de forma directa o a través de una máquina de marcar boletas. Entre los años 1994 y 2003, Venezuela utilizó sistemas de este tipo, basados en un sistema de boletas impresas en papel con un espacio rellenado por el elector y posteriormente contabilizados mediante un sistema de reconocimiento óptico de caracteres.

En principio, estos sistemas resuelven el problema más álgido de la incorporación de tecnología al sufragio: al mantener el principio de que la voluntad del elector se expresa en un trozo de papel anónimo, desacopla el acto de emisión de voto (que debe ser inauditable) del acto de escrutinio (que debe ser auditable en todos sus detalles). De esta manera es posible construir un sistema en el cual todos los resultados en los que la informática está involucrada pueden ser auditados independientemente de los dispositivos usados y el software en sí, mediante el simple recurso de realizar un recuento manual.

Aún así, la aplicabilidad de estos mecanismos no pueden tomarse en forma aislada, sino en el contexto del sistema completo del cual forman parte. Es posible tomar muchas decisiones respecto del sistema como un todo que pueden anular total o parcialmente las ventajas del mecanismo.

Un elemento que no puede faltar en la aplicación de sistemas de recuento automático es la auditoría manual de los resultados arrojados por una porción estadísticamente significativa de las máquinas usadas, seleccionadas al azar luego del acto eleccionario. De lo contrario, una programación maliciosa del software de tabulación de votos podría alterar los resultados sin ser detectada.

Estos sistemas pierden una porción importante de sus ventajas cuando la boleta no es marcada a mano por el elector. Las máquinas de marcar boletas vuelven a introducir en el sistema muchos de los problema asociados con las máquinas de registro directo. Si bien permiten que el votante verifique que las marcas en la boleta se correspondan con sus elecciones, suponen un doble trabajo para el votante (elegir por un lado, controlar por otro), lo que aumenta la probabilidad de que el elector no realice concienzudamente el control. Esto hace factible el mismo ataque que se puede hacer en las máquinas de RED: introducir código que intente adulterar la intención del votante, pero abandonar el intento si el votante rechaza la boleta. De esta manera se pueden secuestrar los votos de todos aquellos ciudadanos que no sean lo suficientemente cuidadosos. También ponen en riesgo el anonimato del voto, toda vez que la máquina de marcar boletas podría agregar, además de las manchas legítimas, algunas que pasen por "suciedad" pero en realidad codifiquen información que permita reconstruir la secuencia de emisión de los votos.

Otro mecanismo que reduce la utilidad de estos dispositivos es el de pasar la boleta por el escáner antes de introducirla en la urna, en vez de hacerlo al abrir ésta. Esto no sólo aumenta los costos (requiere un escáner por mesa, mientras que de otro modo puede utilizarse el mismo escáner para varias de ellas), sino que potencialmente permite registrar la secuencia en la que se emitieron los votos, y así reconstruir la relación de cada votante con su voto.

Una crítica común a este tipo de mecanismo señala la dificultad que presentan en el caso de elecciones complejas, en particular cuando se realiza una elección para múltiples cargos en múltiples niveles de distrito. En una elección en la cual, por ejemplo, se deba elegir concejales de la ciudad, intendente, legisladores provinciales, legisladores nacionales, gobernadores y presidente, la magnitud de la boleta dificulta al votante el marcado de todas las opciones, así como su posterior lectura detallada. Sin embargo, esto es más una crítica de las elecciones complejas que del sistema de recuento automático en sí: mientras más compleja es una elección, más difícil es votar en ella y contar los votos. La "solución" a este problema ofrecida por los sistemas RED consiste, básicamente, en barrerlo bajo la alfombra: como en ellos es imposible contar a mano los

votos, disfrazan el vicio de virtud declarando que es una tarea "innecesaria".

Otra crítica común a estos mecanismos, e igualmente inmerecida, es la que objeta la facilidad con la que se puede alterar o anular un voto mediante el agregado de marcas por parte de quienes realizan el escrutinio. Si bien la factibilidad del ataque es real, es exactamente la misma que con cualquier sistema basado en papel, que a su vez es mejor que la de cualquier sistema completamente electrónico: mientras que las boletas pueden ser alteradas, ésto debe ser hecho individualmente con cada boleta, y el impacto de una persona corrupta se circunscribe a las boletas bajo su custodia. En el sistema electrónico, en cambio, una única persona corrupta tiene el potencial de infectar un gran número de máquinas, comprometiendo de esa manera incluso la integridad de votos en masa, incluyendo los de mesas cuyos fiscales actúen de buena fe.

Sistemas de Registro Electrónico Directo

Los Sistemas RED o DRE son aquellos que más se corresponden con el imaginario popular de las "urnas electrónicas". Representan, además, el modelo preferido de la mayoría de las empresas que participan de este mercado. Las urnas electrónicas usadas en Brasil, así como en varios estados de EEUU o en las últimas elecciones de Venezuela pertenecen a esta clase.

Los sistemas RED se caracterizan por realizar simultáneamente el registro y la tabulación del voto mediante un dispositivo informático que es operado directamente por el votante mediante un teclado, una botonera especial, o una pantalla táctil. Algunos sistemas de RED ofrecen además ayuda para personas con algún tipo de discapacidad, por ejemplo mediante una interfaz de audio para superar las dificultades visuales. A diferencia de los sistemas de recuento automático, en los que el soporte fundamental del voto es la boleta marcada por el ciudadano, en las máquinas RED el registro se realiza directamente en la memoria del dispositivo.

Muchos proveedores de equipamiento señalan como una ventaja del sistema el hecho de que permite "independizar del papel" a la elección. Por lo general, recomiendan no usar la opción ofrecida por algunos modelos de máquinas RED de usar impresoras similares a las que funcionan dentro de las cajas registradoras para generar una cinta de auditoría, argumentando que "desnaturaliza el voto electrónico." En todo caso, las máquinas RED no usan el papel emitido para sus

resultados, sino que se basan enteramente en los registros presentes en su memoria.

Los sistemas RED pueden configurarse de tal modo que permitan al usuario corregir sus opciones y hasta votar en blanco, pero no permiten invalidar el voto ni cometer errores clásicos que resultan en la anulación del voto.

Los sistemas RED suelen ser también los preferidos por aquellos que trabajan en las elecciones, porque son los que más trabajo les ahorran: no hay boletas que custodiar, el recuento de votos es inmediato, y no hay riesgo de que un nuevo recuento de votos arroje una diferencia con el anterior: la máquina obtendrá siempre el mismo resultado, independientemente de si éste refleja la voluntad de aquellos que la usaron para votar o no.

En esta preferencia se hace evidente un punto de tensión entre los intereses de los ciudadanos (que necesitan que el resultado refleje sus elecciones) y los de quienes están encargados de conducirlo (quienes desean terminar la tarea con la mayor rapidez y el menor esfuerzo posible, descargando tanta responsabilidad como se pueda por eventuales errores o actos de corrupción).

SISTEMAS DE VOTACIÓN A TRAVÉS DE INTERNET

También conocidos como sistemas de votación a distancia, son mecanismos para emitir el sufragio desde una computadora común conectada a la red de redes, permitiendo que los sufragantes emitan su voluntad desde sus propios domicilios, desde puntos públicos de acceso, e incluso desde el extranjero. Existen variantes de estos sistemas que permiten emitir el voto no sólo desde una computadora personal, sino eventualmente también desde un teléfono celular o un sistema de televisión digital.

Uno de los desafíos más graves que enfrenta este tipo de sistemas es la identificación del votante, que es imprescindible para asegurar varias propiedades importantes del mecanismo, tales como evitar que alguien vote más de una vez o en nombre de otra persona, o que voten personas que no están habilitadas para hacerlo. Este problema suele resolverse mediante una clave unívoca y personal, que puede incluir elementos físicos de autenticación tales como la posesión de una tarjeta de identificación criptográfica o un generador de claves pseudoaleatorias.

Aún con los métodos de autenticación más sofisticados, no queda claro que sea posible reconciliarlos con los requerimientos de identificación exigidos por la ley, que por

lo general requieren la verificación de documentos de identidad por parte de autoridades electorales. Un problema adicional asociado al de la identificación es que obligan a que la máquina que recibe el voto tenga conocimiento de quién lo está emitiendo. Esto ofrece un punto único de ataque para quien quiera violar el secreto del voto: basta con obtener la información almacenada en el servidor del sistema de votos para averiguar cómo votó cada persona que lo usó.

Los proponentes de estos sistemas señalan que se prestan a ser usados en lugares en los que la participación en las elecciones no es obligatoria y está permitido votar por correo. El argumento es sólido, en el sentido de que es un sistema que puede ser usado en contextos en los que la experiencia muestra que el riesgo de fraude es bajo.

Es interesante señalar que hay experiencias exitosas de uso de votación a distancia en ciertos ámbitos específicos, en particular en aquellos en los que los participantes tienen un grado alto de familiaridad y acceso a recursos informáticos y está ausente la exigencia de anonimato. El proyecto Debian, por ejemplo, un proyecto comunitario de desarrollo de software integrado por personas de todo el mundo que no tienen oportunidad de encontrarse físicamente para votar, utiliza voto a distancia como una herramienta cotidiana, con excelentes resultados. El sistema es robusto, justo y difícil de engañar, pero sólo funciona gracias al hecho de que el voto no es secreto.

Principales problemas detectados

Beatriz Busaniche y Federico Heinz

Los sistemas de voto electrónico (en el sentido usado en este libro) suelen venir de la mano de contundentes afirmaciones acerca de sus virtudes, tales como una mayor transparencia del acto electoral, la eliminación del clientelismo político, la rapidez e infalibilidad del conteo, el menor costo de cada elección, y la mayor participación ciudadana.

Lamentablemente, estas afirmaciones categóricas no vienen acompañadas de datos sólidos que las sustenten, y algunas empresas proveedoras invierten un esfuerzo nada despreciable en evitar que sean verificadas por terceras partes independientes, como fue el caso de Sequoia Systems en 2008, que intentó impedir una auditoría independiente de seguridad encomendada por el estado de Nueva Jersey argumentando que llevarla a cabo violaría los términos de uso del software que controla las urnas[1].

De hecho, ninguna de esas afirmaciones soporta un análisis profundo y, si bien algunas de ellas pueden ser ciertas para algunos casos particulares, la experiencia internacional demuestra que en la realidad están muy lejos de reflejar el verdadero desempeño de las urnas electrónicas.

Transparencia

La afirmación de que las urnas electrónicas aportan a la transparencia del comicio es, probablemente, la más aventurada. Es difícil comprender cómo un proceso opaco se haría más transparente mediante el recurso de agregarle

una “caja negra”. Lejos de aportar a la transparencia, la urna electrónica obstaculiza la capacidad de la mayoría de los ciudadanos de fiscalizar la elección.

Cualquier persona sabe cómo verificar, con sólo mirarla, que una urna está vacía o que un precinto de seguridad está intacto, y el sistema educativo apunta a garantizar que todas las personas sepan leer, escribir y contar. Pero estas habilidades son inútiles a la hora de ver qué pasa "dentro" de una urna electrónica: la inspección ocular no sirve para ver si está vacía sino que es necesario usar un programa diseñado a tal fin, que imprima un ticket que diga "sí, estoy vacía". ¿Podemos creerle?

Cuando la urna imprime los resultados, los obtiene de operar sobre sus registros internos, almacenados en medios magnéticos que los fiscales no pueden leer por sus propios medios. La única "comprobación" posible de que la urna está efectivamente vacía, o de que los totales son correctos, es repetir la operación, la que previsiblemente dará siempre el mismo resultado. Aún si confiáramos en que el programa de la urna es correcto, el fiscal promedio carece de los conocimientos y las herramientas necesarios como para comprobar si el programa que está instalado en la urna ha sido adulterado o no.

Incluso un fiscal con grandes conocimientos de programación y electrónica digital, provisto de herramientas especializadas, probablemente demoraría días en verificar con algún grado de confianza que la urna está efectivamente "en cero", mientras que hacerlo con el mismo grado de confianza con el que puede hacerse inspeccionando el interior de una urna de cartón es efectivamente impracticable: se trata de un problema de la misma complejidad que la construcción de programas de computadora libres de errores, algo que el estado del arte aún no nos permite. Para peor, las acciones que debería realizar este hipotético auditor especializado son mucho más invasivas que las necesarias para adulterar el funcionamiento de la urna, de modo que, suponiendo que nos diga que la urna está "limpia", no sólo no va a poder demostrárselo a alguien que no esté similarmente especializado, sino que no tenemos manera de saber si lo que hizo, en realidad, fue verificarla o subvertirla.

Este es un problema fundamental de las urnas electrónicas: mientras la verificación de su confiabilidad dependa exclusivamente de comprobar que "funciona bien", la tarea de su fiscalización queda necesariamente en manos de una élite tecnológica, a la que el resto de la población no tiene más remedio que creerle. Para corromper la fiscalización de una elección basada en papel, es necesario contar con fiscales corruptos en un número importante de mesas, pero en el caso de las urnas electrónicas basta con sobornar o extorsionar a un grupo pequeño de personas fácilmente identificables.

Estas dificultades a menudo son desestimadas, argumentando que se pueden realizar elecciones de prueba controladas para ver cómo se comporta la urna, y señalando que estas urnas se han usado en muchos lugares sin problemas. Lamentablemente, este argumento ignora el hecho de que es muy sencillo programar la máquina de modo que no se comporte de la misma manera durante las pruebas que durante la elección, y que la experiencia demuestra que en la mayoría de las elecciones, la necesidad de actualizar el software (ya sea el mismo software de la urna o su sistema operativo) lleva a que el programa que corre durante la elección puede no ser el mismo que se usó durante las pruebas.

Por lo demás, la afirmación de que estas urnas han sido usadas sin problemas es harto aventurada: no sabemos si hubo problemas o no, precisamente porque la opacidad del mecanismo no nos permite comprobarlo adecuadamente. Es perfectamente posible que en esas elecciones haya habido problemas masivos, sin que nadie haya podido probarlo y ese es precisamente el escenario que las urnas electrónicas facilitan. De hecho, hay elecciones como las de EEUU en 2004, en las que las diferencias entre las encuestas en boca de urna y los resultados finales sugieren fuertemente que las urnas dieron resultados incorrectos.

El fin del clientelismo

El clientelismo político es un problema social, económico y educativo que no se soluciona con tecnología. Para que la "compra de votos" funcione, es necesario contar con un mecanismo que permita al comprador un grado importante de confianza en que el votante efectivamente votará por el candidato al que prometió votar. En las elecciones en papel, esto puede hacerse a través del denominado "voto en cadena", mecanismo que algunos sistemas de voto electrónico hacen efectivamente imposible.

Pero pensar que el voto en cadena y el clientelismo son lo mismo es un error: el voto en cadena es sólo un mecanismo de romper el secreto del voto. No es el único, y las urnas electrónicas ofrecen mecanismos alternativos potencialmente mucho más eficaces. Esto se debe a la naturaleza fundamentalmente distinta de las urnas electrónicas. Por ejemplo, mientras que las urnas normales son contenedores pasivos, de información, los circuitos de la urna electrónica emiten radiación electromagnética. Experimentos realizados en Holanda demostraron que estas emisiones hacían posible detectar por quién votaba una persona desde una distancia de 25 metros, usando sólo dispositivos disponibles comercialmente.

En el estado de Ohio se descubrió, dos años después de usarlas, una grave falencia en las urnas electrónicas que permite violar el secreto del voto luego de los comicios: los reportes emitidos por la urna al final del recuento permiten reconstruir el vínculo entre voto y votante. Este caso es particularmente grave, porque ilustra un aspecto a menudo ignorado del cálculo de riesgo a la hora de usar una urna electrónica: el hecho de que no conozcamos vulnerabilidades en la urna no quiere decir que no existan, ni que nadie las conozca. Alguien que estuviera en conocimiento de esta vulnerabilidad hubiera podido organizar una compra o extorsión masiva de votos que hubiera sido indetectable y requerido un esfuerzo logístico mucho menor que el voto en cadena.

La rapidez del conteo

Una de las escasas ventajas promocionadas que podría ser verificable es la rapidez en el conteo. De hecho, cuando todo sale bien, los resultados pueden ser inmediatos. El problema surge cuando evaluamos el impacto potencial de las distintas cosas que pueden salir mal. Mientras que en la urna de papel, la influencia de un inconveniente es por lo general proporcional a la magnitud de éste, en las urnas electrónicas un problema muy pequeño puede tener consecuencias muy graves. Esto lleva a que si los resultados de la urna electrónica no son inmediatos, por lo general no se los puede obtener nunca. Por lo general, no hay nada al medio.

El 16 de diciembre de 2007, por ejemplo, se utilizaron cuatro urnas electrónicas de la firma Altec Sociedad del Estado (Río Negro) en la localidad de Las Grutas, en Argentina. Transcurrida la jornada electoral, una de esas urnas arrojó un resultado sorprendente: 0 votos. Fue afortunado que en este caso las urnas hayan llevado registro en papel, porque el registro digital se había perdido completamente, pero aún así el escrutinio demoró horas, porque los votos impresos sobre una tira de papel eran mucho más difíciles de identificar que las boletas originales. La única explicación de la empresa proveedora de la urna fue que "alguien debe haber sacudido la urna".

De la misma manera, existen casos en los que una falla técnica en una urna electrónica produjo que la urna contara miles de votos en mesas en las que votaban sólo cientos de personas, o el reciente caso de Nueva Jersey, en el que los resultados fueron inmediatos, pero el total de votos emitidos no coincidía con la suma de los votos emitidos por partido. ¿Puede decirse que ese resultado es inmediato, cuando en realidad es evidentemente incorrecto?[2]

La rapidez, sin confianza ni seguridad, no sirve para mucho en un proceso electoral. Esta es un área en la que la eficacia (hacerlo bien) debe primar por sobre la eficiencia (hacerlo rápido).

La economía

La idea de que usar urnas electrónicas permite economizar dinero en los comicios ha sido refutada por auditores independientes que la pusieron a prueba. En el Estado de Maryland, por ejemplo entre 2002 y 2003 se compraron 19 mil máquinas de pantalla táctil a la firma Diebold. Para poder concretar la compra, el Estado tomó un crédito de 67 millones de dólares, 44 de los cuales fueron a las arcas de la empresa en concepto de compra y mantenimiento de las urnas. Antes de incorporar estos dispositivos, Maryland usaba un sistema de escaneo óptico.

Según el informe de la organización Save Our Votes, publicado en febrero de 2008[3], el cambio de tecnologías implicó un aumento promedio de 179% en el costo total por votante. En uno de los condados, el aumento fue de 866 %. Por cierto, las máquinas de Diebold aún no se terminaron de pagar y ya deben ser renovadas. El Estado de Maryland está considerando volver al sistema de escaneo óptico.

La participación ciudadana

Un tema crítico a la hora de evaluar la implementación de voto electrónico es la participación ciudadana. Nuestras democracias modernas están golpeadas por el descrédito de las clases dirigentes y la falta de confianza en los sistemas políticos. El halo de modernidad que otorga el voto electrónico parece ser la panacea para entusiasmar a los votantes para participar en los comicios.

Sin embargo, es importante destacar que la incorporación de urnas electrónicas tiene efectos claramente contrarios al objetivo de mejorar la participación ciudadana. Sin ir más lejos, las personas poco afines con los sistemas computacionales serán los primeros excluidos: adultos mayores o personas de escasos recursos, personas con dificultades visuales o con bajísimo nivel educativo que hoy día no requieren mayor preparación para elegir una boleta, ponerla en una urna y emitir su voluntad política, se verán enfrentados a un sistema mucho más complejo para votar.

Pero este no es el único inconveniente. Quizás el mayor de los problemas es que aquellos que hoy auditan las elecciones en nuestro nombre (maestras de escuela, empleados públicos, fiscales de partidos políticos) se verán incapaces de auditar eficazmente un sistema de esta naturaleza. Sólo personas altamente calificadas en ingeniería de software, electrónica y hardware podrán comprender el funcionamiento de estos sistemas. Aún personal calificado en seguridad de sistemas de información se manifiesta incapaz de evaluar, validar y corroborar el funcionamiento correcto de urnas electrónicas. Estos mismos expertos difícilmente se atrevan a firmar a conciencia una certificación de seguridad de las urnas pues no existe método formal de validación que los avale.

Así, la participación real y tangible de la ciudadanía se verá reducida a la confianza ciega en un pequeño número de fiscales informáticos que, aún teniendo amplios conocimientos de la materia, no podrán certificar la validez de un resultado en el que todos los demás tendremos que confiar. Aquellos que tenemos la voluntad política de ejercer nuestro derecho a auditar nos veremos limitados por carecer de conocimientos técnicos, y tendremos que dejar la participación real a una pequeña elite de técnicos autorizados.

Si bien no existen sistemas perfectos, la diferencia de impacto es sustancial. Una mesa de votación tradicional puede registrar inconvenientes y ser anulada. El impacto sobre los resultados globales será mínimo. Sin embargo, un error mínimo en un sistema de votación electrónica puede alterar el resultado de una elección simultáneamente en un gran número de mesas.

PROBLEMAS GENERALES

A todo esto vale agregar que, en la gran mayoría de los casos, los proveedores de urnas electrónicas son empresas privadas cuya composición accionaria deberíamos conocer en detalle antes de confiarles un proceso público y ciudadano como es la emisión del voto. ¿Cuáles serán los mecanismos para auditar a las empresas proveedoras? ¿Cómo sabremos cuáles son sus vinculaciones políticas y sus intereses en cada elección? ¿Estamos dispuestos a privatizar un proceso ciudadano como el acto de votar? Estas preguntas surgen a la luz de escándalos ocurridos en los EEUU donde, por ejemplo, uno de los principales

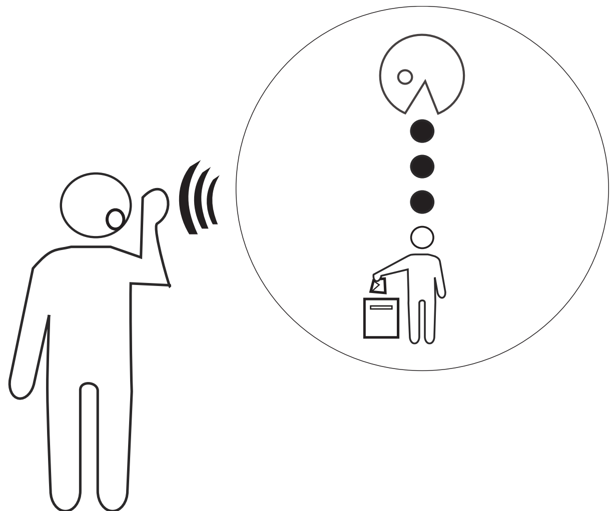
accionistas de una de las empresas proveedoras de urnas (ES&S) resultó ser un senador republicano con obvios y marcados intereses en el resultado electoral.[4]

No son pocos los inconvenientes que aparecen a la hora de evaluar la automatización de la emisión del voto. Sin embargo, es muy poco lo que se discute y ciertamente escaso el conocimiento sobre los mismos. El acto de votar es lo suficientemente importante como para que nos ocupemos de este tema, y nos preocupemos frente a incorporaciones acríticas de tecnología que, lejos de mejorar nuestras democracias, son amenazas al derecho esencial de la ciudadanía a votar en condiciones de secreto, transparencia y seguridad.

Notas

1-http://freedom-to-tinker.com/blog/felten/interesting-email-sequoia
2-http://freedom-to-tinker.com/blog/felten/evidence-new-jersey-election-discrepancies
3-http://www.saveourvotes.org/legislation/2008/08-costs-mdvotingsystem.pdf
4-http://www.scoop.co.nz/stories/HL0301/S00166.htm

voces



Se cayó el sistema

El pedregoso camino del voto electrónico en Las Grutas (Argentina)

Este texto es fruto de la entrevista realizada por Beatriz Busaniche (Fundación Vía Libre) con la edil María Liliana Gemignani, concejal de San Antonio Oeste que fue una de las primeras en dar la voz de alerta ante los problemas del sistema de Voto Electrónico implementado por la empresa ALTEC S.E. en una prueba piloto en una elección vinculante en el Balneario Las Grutas el 16 de diciembre de 2007. Gemignani, junto a los ediles Ojeda y Fernández son los autores de la ordenanza derogatoria que reproducimos en el anexo de esta publicación.

Sobre finales de año 2007, el correo de contacto de Fundación Vía Libre recibió un mensaje del periodista de Las Grutas Sergio Ploss en el que solicitaba ayuda ante la inminencia de una implementación de Voto Electrónico en su lugar de residencia, donde se planificó el uso de urnas electrónicas de la firma estatal rionegrina ALTEC S.E. Tras la aprobación unánime de una ley provincial, se había resuelto que Las Grutas fuera el primer lugar de implementación de estos sistemas en cuatro mesas, dos femeninas y dos masculinas, en votaciones obligatorias y vinculantes para autoridades municipales.

Unos doscientos ciudadanos, encabezados por el propio Ploss, presentaron un recurso de amparo ante la justicia en reclamo de su derecho a votar en condiciones tradicionales, más este recurso fue rechazado un día antes de la elección bajo el argumento de que estaban dadas las condiciones de seguridad para realizar el comicio. La baja en la tasa de votantes, los problemas ocurridos en la jornada y la falta de garantías para que la ciudadanía ejerciera su derecho al voto universal y secreto fueron los detonantes para que la Concejal Gemigniani reclamara la

derogación de la ordenanza que finalmente fue aprobada por unanimidad.

Este es el diálogo que mantuvimos con la Concejal sobre el por qué de la necesidad de dar marcha atrás y lo que puede compartir de esta experiencia con quienes están evaluando incluir voto electrónico en los procesos electorales en otras ciudades argentinas.

Beatriz Busaniche: ¿Desde cuándo tienen voto electrónico en la provincia de Río Negro?

María Liliana Gemignani: Desde que se aprobó por ley 4082[1] en la Provincia.

BB: ¿Cuál ha sido el argumento para aprobar una normativa de este tipo?

MLG: El argumento estaba basado en la seguridad, y en especial se hacía hincapié en que de esta manera era más difícil manipular el voto con las artimañas que se acostumbran a hacer en los comicios: darles la boleta antes de entrar, el voto cadena u otra manipulación similar. Consideraban que era necesario modernizar el sistema y que daba mayor seguridad en el acto eleccionario.

BB: ¿Quiénes lo promocionaban?

MLG: Fue una ley presentada por el bloque del oficialismo provincial, pero la apoyaron todas las bancadas políticas de la Legislatura Provincial. Luego el bloque oficialista del Concejo Deliberante de San Antonio Oeste de Concertación Cívica presenta el proyecto de Ordenanza adhiriendo a la ley en el ejido municipal para las próximas elecciones de diciembre de 2007 y fue aprobada por unanimidad. Además cabe aclarar que todos los partidos participantes de la última elección decidieron que como primera experiencia, se aplicara en el 50% de las mesas electorales del Balneario Las Grutas. Creo que todos en un primer momento pensaron que era bueno.

BB: Ante la primera prueba piloto realizada en Las Grutas, en diciembre de 2007, ¿considera que las promesas sobre las que se fundó la normativa de voto electrónico en la provincia se cumplieron?

MLG: Para nada, porque todo funcionó muy mal. Las dos mesas femeninas fallaron, sólo una mesa masculina

funcionó regularmente. Al comienzo del comicio vinieron autoridades provinciales y de la empresa Altec que las construyó, a inaugurar el acto eleccionario como algo histórico ante la prensa. Pero cuando empezaron los problemas no apareció nadie y los técnicos de la empresa no tuvieron respuestas, sólo que era un “error de sistema” y que no entendían cómo si habían cargado el padrón en la máquina tal cual el padrón de papel, existían estas ausencias. Sólo la Junta Electoral Municipal, que no sabía muy bien qué hacer y los miembros de los partidos políticos, tuvieron que hacer frente a la problemática.

BB: Sabemos que ante la perspectiva del uso de voto electrónico en Las Grutas, un buen número de votantes de esa localidad presentaron un recurso de amparo para votar de manera tradicional. Ese amparo fue rechazado. ¿Cuáles fueron los argumentos para rechazarlos? ¿Y cuál fue la reacción de los diferentes sectores políticos cuando se presentó ese amparo?

MLG: En realidad todo comenzó por el señor Sergio Ploss, dueño del semanario El grutense, que inicia una campaña y pone en conocimiento a la población sobre el peligro del voto electrónico y se realizan algunos recursos de amparo y se organiza una exposición por parte de Iván Santander de la Fundación Vía Libre. En esa oportunidad varias facciones políticas que se presentaban en esa elección manifestaron su rechazo al sistema y lo plasmaron en un documento, menos el partido que representaba al oficialismo local y provincial. La respuesta a los recursos de amparo fue recibida el día anterior y no reconocía que no estuvieran las condiciones dadas y tampoco consideraban discriminatorio el hecho que sólo un sector del padrón electoral de Las Grutas votara con este sistema, mientras todo el ejido municipal restante lo hacía de forma tradicional.

BB: ¿Podría sintetizar qué ocurrió el 16 de diciembre cuando se realizaron las elecciones a intendente usando cuatro urnas electrónicas en las Grutas?

MLG: Si bien trajeron unos días antes las máquinas para que la gente practicara, no fue mucha la gente que concurrió a hacerlo. Pero los problemas que se sucedieron no fueron por culpa de la inexperiencia de la gente sino de errores en las máquinas. En las mesas femeninas de voto electrónico, se presentaban a votar y no aparecían en el padrón ingresado en la máquina, pero sí en el de papel que utilizaban los fiscales para su control. Casi se quedan sin

votar y por pedido de los partidos y de la Junta electoral municipal se los anotaba a mano en las otras mesas femeninas de voto tradicional y votaban allí, generando grandes demoras y mucho trabajo por parte de los fiscales que debían tomar nota de los datos de los votantes, a mano. En una mesa masculina se terminó el papel y las máquinas se abrieron, perdiendo su carácter de inviolable. También un señor le planteó a un fiscal que el papel no se había cortado y había visto a quien había votado la persona que pasó adelante de él. Y lo más trágico fue cuando se cerraron las mesas y en una mesa masculina electrónica la máquina se tildó y emitió un papel que daba 0. Hubo que custodiar la máquina con la policía por horas, por miedo a que se cometiera fraude y se abrió a la noche cuando ya se había terminado hacía dos horas el comicio. Se tuvieron que contar los papelitos de adentro de la máquina a mano. Todo fue más lento y por momentos muy desesperante.

BB: ¿Cuál fue la reacción de la gente ante los problemas?

MLG: Se enojaba y reclamaba. Cuando se dio el primer problema de una señora que no aparecía en la máquina la mandaban a su casa sin votar, pero realizó el reclamo y se empezó a implementar lo relatado anteriormente.

BB: Sabemos que usted ha sido una de las impulsoras de la derogación de la ordenanza de voto electrónico para San Antonio Oeste y Las Grutas, ¿nos puede contar en qué se basó para impulsar esta derogación y cuál fue la reacción de las fuerzas políticas involucradas?

MLG: Yo en realidad tenía mis dudas con el sistema, en especial creía que debía haberse implementado opcional, porque mucha gente mayor o que no tiene acceso a la informática se iban a negar a ir al acto eleccionario. Pero cuando vi el material que trajo Iván Santander, de la Fundación Vía Libre, realmente me preocupé. Realizamos con algunos vecinos un manifiesto con junta de firmas para evitarlo. Cuando sucedió todo lo expuesto anteriormente, creí que en mi carácter de concejal debía hacer algo y con los miembros de mi interbloque "JUNTOS", los concejales Luis Ojeda y Mónica Fernández, presentamos un proyecto de Ordenanza derogando la adhesión al voto electrónico basado en lo que sucedió y en el dictamen de la Junta electoral municipal. Además de haber sido partícipe de todos estos acontecimientos. Fue votado por unanimidad en el Concejo Deliberante, pero plantearon que lo hacían por todos los errores que sucedieron, aunque creían en el mejoramiento del sistema.

BB: ¿Qué va a pasar en las próximas elecciones?

MLG: Se tienen que realizar las elecciones en la forma tradicional.

BB: Como concejal con experiencia en una implementación de voto electrónico, ¿Qué le diría a sus colegas de otras ciudades que evalúan avanzar en la incorporación de estos sistemas al régimen electoral (como la Ciudad de Buenos Aires, por ejemplo).

MLG: Que todos los argumentos esgrimidos sobre la rapidez, economía, seguridad e inviolabilidad del voto, se caen rápidamente cuando se pone en práctica. Que se corre un riesgo muy grande de perder el secreto del voto, porque existen formas de corroborar a quien se votó, que las máquinas se pueden descomponer y generar todos los problemas que nosotros vivimos. Que el sistema tradicional es fácil y seguro y no requiere mantenimiento. Pero por sobre todas las cosas tengan en cuenta que las personas mayores y aquellos que no han tenido acceso a las computadoras se sienten discriminadas y no concurren a votar por temor a equivocarse o por vergüenza. Y el **elegir a las autoridades en libertad es un derecho que nos costó mucho a los argentinos y que debemos defenderlo.**

Notas

1- NdE: La Ley Nº 4082 Sistema de Voto Electrónico fue sancionada el 18/05/2006 y promulgada el 01/06/2006 por Decreto Nº 496/2006 publicado en el Boletín Oficial del 15/06/2006 Pag.1. Entrada en vigencia el 23/06/2006

Las voces de alerta

Cómo fue la organización de la ciudadanía ante el voto electrónico en Las Grutas

Este texto es fruto del diálogo mantenido por Iván Santander con Beatriz Busaniche, para documentar las acciones realizadas por un grupo de ciudadanos ante la perspectiva de tener que usar urnas electrónicas en las elecciones del 16 de diciembre de 2007 en Las Grutas.*

Cuando el periodista Sergio Ploss se comunicó con Vía Libre para solicitar apoyo en una acción jurídica contra la implementación de Voto Electrónico, apelamos a los colaboradores más cercanos al lugar de la experiencia. Iván Santander, miembro del Grupo de Usuarios de Software Libre del Alto Valle se ofreció a participar de las actividades y la campaña que se estaba armando en el Balneario Las Grutas para alertar a la ciudadanía sobre el riesgo del Voto Electrónico. Él mejor que nadie puede contarnos lo que ocurrió en esas semanas en las cuales la gente trató de evitar lo que parecía inevitable, el uso de urnas electrónicas en una elección obligatoria y vinculante.

BB: Iván, ¿Cuándo tomaste conocimiento de que se iba a realizar una experiencia de voto electrónico en Las Grutas?

IS: Fue por medio de la lista de amigos de Vía Libre[1], prácticamente al mismo tiempo comenzaron a aparecer artículos en el Diario de Río Negro. Fue un tema al que se le dio poca difusión periodística. Sólo cuando empezamos a movilizarnos aparecieron algunos periodistas que nos escucharon. Debo agradecer al periodísta Hugo Alonso,

quién tuvo la amabilidad de hablar conmigo por teléfono y publicar una nota en el diario Río Negro, donde anunciaba la charla que iba a dar y el malestar de la población.

BB: ¿Qué pasa en el resto de la provincia, cuál es la situación jurídica hoy?

IS: A nivel provincial no hay cambios, tenemos todavía una ley que es provincial y está vigente. Es de esperar que para las elecciones a gobernador quieran hacer uso de esta tecnología, seguramente no será a gran escala porque las experiencias que han tenido hasta el día de hoy no han sido muy buenas, y creo que las próximas elecciones serán muy peleadas. No creo que quieran incorporar una variable más de deserción de votantes o autoridades de mesa.

BB: ¿En qué basan sus argumentos los promotores del voto electrónico?

IS: Los argumentos son siempre los mismos, muletillas del tipo: "¿cómo en una era super informatizada vamos a seguir usando cajas de cartón y papeles para votar? Nos promenten una tecnología que aumentará el secreto y universalidad del voto, que aumentará la participación ciudadana gracias a esta extraordinaria tecnología. Desgraciadamente en Río Negro las cosas se han hecho peor que en otros lugares, ya que no se invitó a ninguna empresa con experiencia a mostrar sus productos. Simplemente se hicieron los pases mágicos para que Altec SE[2], que aparentemente fabrica muy buenos parquímetros, se hiciera cargo de fabricar dichos equipos. Y los resultados eran los de esperar, un rotundo fracaso que se intentó minimizar por todos los medios.

Tampoco existe una posibilidad de dialogar con las autoridades para acercarles propuestas, el ministro de gobierno sólo repite siempre el mismo discurso sin fundamento alguno, y la presidenta de Altec compara máquinas de votación con cajeros automáticos. Veo muy difícil hacerles entender los problemas que irremediablemente van a surgir, de hecho hicieron caso omiso a lo sucedido en Las Grutas. Y no es de extrañar que sea así, el negocio es más que interesante económicamente hablando.

BB: ¿Cuál fue la reacción de la gente en Las Grutas? ¿Cómo fue lo del Recurso de Amparo? ¿Qué resultados se obtuvo por esa vía?

IS: En forma mayoritaria la gente estaba en contra, y eran muchos los motivos. El primero era político, desconfianza hacia la autoridad provincial. De hecho, de todos los candidatos a intendente, el único que estaba a favor era el representante de la UCR. Todos los otros, incluido Iud que como legislador votó a favor de la implementación del voto electrónico, estaban en contra de la utilización en forma obligatoria.

El recurso de amparo no prosperó mucho, fue presentado por un periodista de Las Grutas que se sintió discriminado por tener que utilizar un medio que le resultó altamente desconfiable. Desgraciadamente rechazaron el recurso, y el circo siguió adelante con el aval de la justicia.

BB: Si tuvieras que darle un par de recomendaciones a un legislador que esté pensando en implementar voto electrónico, y tras la experiencia de Las Grutas, ¿qué le dirías?

IS: Quizás la principal recomendación sería tomar la incorporación del voto electrónico con la seriedad que se merece. Es obvio que en un futuro la tecnología habrá avanzado lo suficiente como para poder incorporar mejoras al proceso de votación. Pero se necesita generar debate con expertos en la materia, siempre que hablan de "asesores" o "facultativos" no son precisamente informáticos. Son contadores o abogados. Es como si habláramos de medicina con arquitectos o ingenieros y dejáramos de lado a los médicos. Si la idea es implementar sí o sí el voto electrónico, que arbitren todas las medidas necesarias para que sea lo más serio posible y dejen abierta la posibilidad de que quienes desconfían tengan la oportunidad de usar el método tradicional.

BB: ¿Qué nos depara el futuro en Río Negro? ¿Seguirán adelante con la implementación de voto electrónico o se prevén medidas como la derogación de la ordenanza en SAO Y Las Grutas?

IS: Hace poco hubo una nueva experiencia en Viedma, se incluyeron algunas mejoras como por ejemplo la exclusión del padrón electoral de la urna[2]. El padrón estará impreso en papel, el proceso aparenta ser similar a la votación como la conocemos hasta ahora. La primera pregunta es ¿entonces qué resuelve la urna electrónica? un conteo más rápido, nada más. Pero se deberá seguir manteniendo la misma estructura de hoy en día: autoridad de mesa y fiscales. Entonces nos quedamos con una tecnología totalmente inútil, es como si para crear un documento de texto usáramos una computadora para escribir y corregir el texto, pero para llevarlo al papel nos

viéramos forzados a usar papel y lápiz. Si la idea es utilizar una máquina que solamente cuente los votos, están reinventanto la rueda. Se podrían utilizar tecnologías de reconocimiento óptico como las utilizadas en otras partes del mundo.

Notas

1- NdE: Refiere a una lista de correos interna de la Fundación Vía Libre en la que se planifica el trabajo que realiza la organización junto con colaboradores y miembros amigos.
2- NdE: Para la misma fecha de realización de esta entrevista (28 de septiembre de 2008), el Diario de Río Negro publica el artículo titulado "Cosmética para las urnas electrónicas - Se utilizarán en las elecciones de una junta vecinal de Viedma".
"Las elecciones de renovación de autoridades en la Junta Vecinal del barrio Santa Clara de esta ciudad servirán para ir puliendo el mecanismo de voto electrónico en la provincia de Río Negro. Las urnas desarrolladas por la empresa estatal Altec presentarán cambios con una manipulación distinta, similar a un cajero electrónico, y más ágil, dado que no tendrá cargado el padrón que pondrá en discusión el futuro de ese organismo comunal. Será más simple dado que los cambios permitirán armar las listas por categoría electoral, como si se tratara de una 'playstation' que permite al que la usa armar un equipo de fútbol a su gusto", contó a "Río Negro", el presidente de la Junta Electoral capitalina, Hugo Gordillo. La minimización de operaciones que evitarán un momento de tensión entre los electores tendrá por característica que el padrón no estará en la urna electrónica. Se estableció que el presidente del comicio tenga el listado de votantes en planillas de papel, y a medida que los votantes concurran al lugar del comicio, se certificará su presentación y luego podrá concurrir al cuarto oscuro apretar el botón de opciones. (...)"
Fuente: Diario de Río Negro. 21 de Septiembre de 2008. En línea (última visita 30/09/08) en
http://www.rionegro.com.ar/diario/2008/08/21/20088r21s13.php

* Sobre el autor

Iván Santander es Administrador de Sistemas en la Municipalidad de General Roca, Provincia de Río Negro. Es miembro colaborador de Fundación Vía libre además de fundador del GUSLAV, Grupo de Usuarios de Software Libre del Alto Valle. Es un viejo militante del Software Libre en su provincia donde ha dado charlas, cursos y seminarios sobre Software Libre desde los aspectos tanto técnicos como filosóficos. Desde el 2008 ha iniciado además la firma INNOVA Soluciones Informáticas con Software Libre.

Los votos intangibles llegaron al sur

Ushuaia, la ciudad más austral del mundo, tiene en Argentina otro hito: es la primera ciudad que utilizó sistemas de voto electrónico en una elección vinculante en el país. Allá por el año 2003, la clase política de la ciudad se posicionaba como la más avanzada en materia de incorporación de nuevas tecnologías al proceso electoral gracias a la gentileza de la firma española Indra, que puso a disposición equipamientos de votación en forma gratuita para las elecciones municipales. Desde entonces, la historia ha tenido idas y vueltas, incluyendo la imposibilidad práctica de cumplir recaudos mínimos de seguridad y un posterior regreso a las elecciones en papel para el año 2007.

Marcelo Papuccio y la Fundación Apertura Digital en Ushuaia siguieron de forma permanente estas idas y vueltas y mantuvieron la voz ciudadana firme contra la desmaterialización total del voto de los ciudadanos de Ushuaia. Hoy nos cuentan cómo fue esa historia.

Beatriz Busaniche: ¿cuándo y cómo comenzó el uso de voto electrónico en Ushuaia?

Marcelo Papuccio: Comienza en 2003 como una iniciativa del Intendente Garramuño a partir de una propuesta de INDRA en la cual no se cobraba el servicio de alquiler de las urnas, aunque sí el traslado, instalación, asesoramiento, etc.

BB: ¿Cuáles son los argumentos que usan sus promotores?

Los argumentos más usados se basan en un potencial menor costo que el papel, en que es mas simple de utilizar y

no permite algunas trampas como el voto cadena, etc. El Intendente buscaba dar una imagen de modernidad y transparencia.

BB: ¿Qué sistemas usaron en 2003? ¿Cuáles fueron los acuerdos hechos con la empresa proveedora (Indra)?

MP: No conozco los acuerdos específicos, pero el pliego de licitaciones indicaba la necesidad de contar con impresoras en cada máquina que no fue cumplida. Los sistemas usados eran de tipo RED, de Registro Electrónico Directo del voto.

BB: ¿Qué sistemas de auditoría usaron? ¿Cuál fue el rol de la ciudadanía en esos procesos?

MP: Como auditoría consideraron suficiente entregar algunas urnas a instituciones para comprobar su funcionamiento. No se previó una auditoría del software ni del hardware que se utilizó. Cuando insistimos en una auditoría de software la respuesta fue que ya no había tiempo.

BB: ¿Existió algún tipo de oposición o advertencia sobre el uso de voto electrónico?

MP: Prácticamente no hubo oposición, desde Apertura Digital enviamos notas al Concejo Deliberante y mantuvimos reuniones con su Presidenta pero no tuvimos eco (NdE: las dos notas enviadas están en las páginas siguientes en esta misma publicación). La más importante ONG en temas políticos, Participación Ciudadana, impulsó su utilización.

Cuando INDRA reconoció que pondría impresoras en menos del diez por ciento de las urnas hubo algunas voces en contra pero parecieron desubicadas, el Voto Electrónico era lo moderno, lo nuevo, lo mejor.

De hecho si vamos a evaluar políticamente el voto electrónico, se puede decir que tuvo un éxito abrumador. Tanto desde el punto de vista político como desde la ciudadanía, todos estuvieron conformes y contentos. Estar en contra era apoyar la posibilidad del fraude (voto cadena), querer volver al pasado, etc.

BB: En 2007, entiendo que los concejales se pusieron firmes con la necesidad de tener un respaldo en papel para todos los votos. ¿A qué se debió esta actitud de cautela?

MP: El año pasado nos convocaron desde un bloque del Concejo Deliberante y expusimos las fortalezas y debilidades del sistema. Como el Poder Ejecutivo de la Ciudad tenía decidida su utilización y nuevamente no había tiempo para auditar el software, acordamos insistir en dos puntos, que se cumpla el pliego respecto de que cada equipo debía contar con una impresora que permitiera que el ciudadano vea el voto antes de emitirlo y ajustar el costo final al presupuesto establecido.

No pudieron sostener el Pliego Licitatorio que ellos mismos presentaron y que tenía errores terribles como no solicitar las auditorías ni nada. Ninguno de los puntos pudo cumplirse por lo que se decidió volver a usar el voto papel.

BB: ¿Qué está pasando actualmente con las iniciativas de voto electrónico?

MP: Nada, el negocio no funcionó. Cada vez que se habla de implementarlo un funcionario viaja a Buenos Aires a consultar cuánto salen las urnas y la implementación del sistema en lugar de primero pensar y crear un andamiaje legal que lo sustente.

BB: Si tuvieran que hacer alguna recomendación a un legislador que esté evaluando la implementación de voto electrónico, ¿qué le dirían?

MP: En primer lugar que voten una ley que establezca las garantías que debe ofrecer a la ciudadanía el voto electrónico, luego recién salir a hablar con las empresas, no crear una ley basándose únicamente en la oferta existente, que es lo que se ha estado haciendo hasta ahora, al menos aquí en Ushuaia.

Anexo

A continuación publicamos las notas enviadas por Marcelo Papuccio y la Fundación Apertura Digital al Concejo Deliberante de la Ciudad de Ushuaia. Estas misivas no obtuvieron ningún tipo de respuesta.

Ushuaia, 12 de agosto de 2003

Sra. Presidenta del Concejo Deliberante
Doña Mónica Ojeda
S / D

Me dirijo a Ud. a efectos de hacerle llegar algunas apreciaciones respecto de la utilización de urnas electrónicas en las próximas elecciones municipales que han tomado estado público.

Al respecto quiero dejar aclarado que me entusiasma la utilización de esta tecnología, siempre y cuando se tomen los recaudos necesarios para garantizar la transparencia de la elección.

Las consideraciones expuestas a continuación incluyen algunas de las que han surgido con motivo de la implementación del voto electrónico en la Provincia de Buenos Aires.

Consideraciones a tener en cuenta al implementar el voto electrónico

• Es impensable construir la trama jurídica para habilitar el voto electrónico en unos días, o aún peor, si se lograra sería una "Caja de Pandora", como revivir fraude electoral, pero "tecnologizado".

• La legislación Argentina no tiene un adecuado contexto normativo referido a los delitos informáticos. El desvío de votos sería tan fácil como "Incomprobable".

• Se requiere contar con un esquema legal no sólo en lo electoral puro, sino también en lo delictual, y definir la cadena de procesos desde la forma de emitir el voto, pasando por la fiabilidad y auditabilidad del sistema, hasta la familiarización y disponibilidad de los resultados para todos los ciudadanos.

• Aunque nos presten las urnas debemos tener en cuenta como primordial la seguridad y la transparencia del comicio.

• El código fuente de todo el software involucrado en los procesos eleccionarios debería estar abierto a la inspección de expertos

confiables, tanto independientes (ONG, Universidades) como de los partidos políticos interesados, y de igual forma por la ciudadanía en general.

• En el modelo adoptado por Brasil el software usado pertenece y fue desarrollado por el Tribunal Superior Electoral, un organismo del estado (el cual lleva un largo proceso de auditoría por parte de los actores involucrados) y no por una empresa ajena al estado.

• Todo sistema de transmisión crea un desperfecto de seguridad. (Axioma)

• Los fabricantes de las urnas no muestran públicamente el código fuente del software que las hace funcionar y mucho menos de sus planos técnicos amparándose en derechos de propiedad intelectual poniendo el interés corporativo por encima de los derechos de los ciudadanos.

• ¿Cómo puede la justicia garantizar que no existirán registros que permitan vincular la identidad de una persona con su voto?

• ¿Existen garantías de una no manipulación tecnológica?

• Hay cuestiones legales, tecnológicas y de instrucción a la población.

• Debería aprovecharse la cuestión tecnológica del voto electrónico como una estrategia de Estado para aprovechar recursos humanos y de tecnología argentinos.

No tengo ninguna sospecha ni referencia negativa respecto de la empresa Indra, pero el proceso debe ser y parecer lo suficientemente claro como para poder evitar cualquier planteo de irregularidades o incluso de fraude.

Ante esta situación creo necesario replantearse su utilización en esta oportunidad y encarar la tarea de reformar la legislación Provincial adecuándola y creando los mecanismos de control adecuados para garantizar el proceso eleccionario.

Para finalizar quiero citar al Senador Provincial de la Provincia de Buenos Aires Alberto Conde cuando en su fundamentación dice: "Para que sea una alternativa segura y realmente efectiva, el voto electrónico debe cumplir con una garantía fundamental: impedir la alteración de los resultados. Si el Software utilizado por la urna electrónica no es diseñado, probado y publicado en modo de código fuente, al igual que el usado para el recuento de votos, la seguridad no está garantizada"

Quedando a su disposición, saludo a Ud. con la mayor consideración.

Marcelo Papuccio

DNI 13804034

Ushuaia, 19 de agosto de 2003

Sra. Presidenta del Concejo Deliberante
Doña Mónica Ojeda
S / D

Me dirijo a Ud. a efectos de hacerle llegar algunas recomendaciones a partir de la reunión del día 14 entre los Concejales, la Justicia y la empresa INDRA.

De acuerdo a lo conversado con los participantes y acordado con la empresa Indra quedaría por estipular los mecanismos que garanticen los siguientes puntos expuestos para garantizar aún mas la transparencia de la elección:

• La Justicia Electoral deberá definir el contenido de los menúes de selección del software utilizado por las urnas electrónicas y los procedimientos complementarios lo antes posible.

• Los Partidos Políîticos participantes deberían nombrar un Fiscal especial (Informático o Tecnológico) que audite el software y los procedimientos informáticos y de comunicaciones.

• El software no debe permitir efectuar algún tipo de proceso que permita vincular el voto con el votante, al efecto el software debe únicamente acumular el voto.

• Excepcionalmente podría existir el caso especial de los impugnados, y solamente permitir su vinculación temporal en este caso, para lo que debería de estudiar los precedimientos a realizar.

• La empresa Indra debe suministrar a la Justicia Electoral, Partidos Políticos y ONG interesadas los fuentes del software a utilizar el día del comicio al menos quince días antes del mismo para efectuar la auditoría de software correspondiente, otorgando a los mismos un plazo no menor a los 7 días para efectuar los reclamos correspondientes.

• La compilación del software y su grabación en compact flash junto con los datos propios de esta elección que serán ingresados en las urnas electrónicas deberán ser ante la presencia de los fiscales que los partidos designen, y a partir de ese momento las urnas deberán permanecer en custodia.

• La impresión de las actas de cada mesa (urna electrónica) deberá realizarse mediante impresoras de matriz de puntos, chorro de tinta o láser debido al degradado que se produce en las de impresión térmica.

• Debe prestarse atención en el acto de efectuar el voto en la urna electrónica mediante la inclusión de una señal sonora o visual

efectuada por la urna electrónica que permita a las autoridades de mesa verificar el voto.

• Las tarjetas compact flash utilizadas en las urnas deberán ser debidamente identificadas y permanecer en custodia por parte de la justicia durante el período de impugnaciones posteriores al comicio.

Sin otro particular y quedando a su disposición, saludo a Ud. muy atentamente.

Marcelo Papuccio
DNI 13804034

"Un cambio de este tipo requiere consensos muy profundos"

El legislador del Bloque Igualdad Social, Martín Hourest, es una de las voces de la legislatura de la Ciudad de Buenos Aires que ha llamado a la reflexión y el debate antes de avanzar en la implementación de voto electrónico para los procesos electorales. Fue además, junto con sus asesores, parte de la organización de la jornada de debate realizada en la Legislatura de la Ciudad el 30 de mayo de 2008.

En diálogo con Vía Libre analizamos los diferentes escenarios en los que se encuentra la discusión sobre la incorporación de voto electrónico en el marco de la Ciudad Autónoma de Buenos Aires y las posibilidades reales de avance en esta materia.

BB: ¿Cuál es la situación y el actual panorama en relación a los proyectos de ley de voto electrónico en la ciudad?

MH: El proceso de incorporación de voto electrónico en la ciudad está en veremos. Al menos en lo que hace a la agenda del oficialismo, se puede apreciar que el macrismo comenzó su gestión con algunos golpes de efecto fuertes, tales como la extensión de los servicios de subterráneos, las mejoras edilicias en las escuelas, los sistemas de compra en hospitales y la reforma política circunscripta al voto electrónico. De esa agenda, prácticamente todos los temas centrales que interesan a la ciudadanía se han caído o están parados.

En ese contexto, el operador más visible del tema de voto electrónico, Cristian Ritondo, está ahora trabajando más enfocado en las cuestiones que tienen que ver con gestión de basura y residuos en la ciudad.

Esta perspectiva hizo que la presión sobre la comisión de asuntos constitucionales de la legislatura, que es la comisión que tiene que dar despacho favorable a una iniciativa como ésta, se reduzca bastante hasta casi paralizar el debate.

En este sentido, se tiene que dar esta discusión en el marco de los temas centrales para la política en la ciudad como son la ley electoral, la ley de partidos políticos y la ley de financiamiento de la política. Sin estos temas en el tapete, nos negamos a considerar el tema del voto electrónico en sí mismo.

Vale mencionar que la comisión que trata estos asuntos no tiene mayoría del PRO ni de sus aliados. En la lógica de algunos políticos, la discusión sobre el código electoral está inmersa en la discusión más amplia de la ley de partidos políticos y la ley electoral para la ciudad, pero el código electoral es una cosa específica y como tal hay que tratarlo.

BB: Toda vez que se habla de voto electrónico, se lo pretende mostrar como solución a problemas de la política, ¿pero qué problemas se trata de solucionar o al menos cuál es la versión oficial al respecto?

MH: No creo que quieran solucionar ningún problema en particular. Aquí se trata de una pelea por una imagen, que remite a inconvenientes que no necesariamente pasan en la ciudad de Buenos Aires. Algo preciso como ausencia de fiscales y boletas que sí puede tener que ver con la situación a nivel nacional, donde, por ejemplo, lo primero que nos viene a la mente es lo que pasó en la Provincia de Córdoba o en la Provincia de Buenos Aires.

El caso más notable, si se quiere más visible, en la Ciudad de Buenos Aires es la famosa historia del escrutinio, cuando fueron las elecciones que enfrentaron a Cavallo e Ibarra. Pero este hecho no tiene registro en términos ciudadanos, es decir, la gente no se acuerda de eso, sí se acuerda de lo que pasó en Córdoba o en Provincia. Y es a eso específicamente a lo que el macrismo remite cuando habla de voto electrónico. Ellos plantean la idea de que si Buenos Aires es un distrito que no tiene los mismos problemas que el resto de los distritos del país con menos cultura cívica (o al menos con menos de lo que la ciudad cree que tiene), por qué no dar aquí mismo este avance fundamental que según ellos garantiza transparencia, ausencia de manipulaciones, celeridad.

En su orden de argumentos lo que prima es la celeridad, la ausencia de manipulaciones y la transparencia.

BB: ¿Cómo se ha planteado la discusión alrededor de esto?

MH: El gobierno de la ciudad organizó un seminario, el VotoBit[1], pero de ese evento a esta parte no intentaron dar ningún tipo de discusión racional sobre el voto electrónico. Cuando hablan del tema ofrecen una serie de ventajas sin demasiado fundamento, las ventajas son porque sí, son razones del tipo "nadie desconfía del cajero automático" y cosas por el estilo. Se han parapetado detrás de afirmaciones de ese tipo. Incluso, vale mencionar que algunas ONGs que originalmente estaban a favor del voto electrónico, tampoco se han sumado en apoyo de este proyecto.

La gente de Clutterback por ejemplo, que trabajan en transparencia política y sistemas electorales, solía recomendar voto electrónico, pero ahora ni siquiera están alineados en el marco del proyecto que auspicia el macrismo.

Lo que no sabemos con claridad es si se está haciendo algún tipo de prueba piloto o avance en el proyecto. En algún momento dijeron que se iba a ir paso a paso, probando en escuelas, sindicatos, pero no hemos tenido noticias públicas de que algo de eso se esté haciendo.

BB: ¿Cuál es la 'mística' detrás del discurso del voto electrónico que hace que sea tan amigable para la sociedad?

MH: El voto electrónico está instalado en el imaginario de la gente como el mecanismo para la eliminación del aparato político. Virtualmente, la gente cree que al eliminar el aparato se puede volver a creer en la política. Existe toda esta cosa denotativa del puntero, el pensamiento de que el puntero es una línea de falla entre el Estado y la Sociedad Civil. Que el puntero tenga la miseria de intercambiar afiliación por favores, no implica que ese lazo no debería ser reconstituido desde la órbita del derecho y no desde la dádiva.

La gente que va al puntero y le pide un favor, el puesto para el hijo, la cama en el hospital, el turno para el trámite, el plan social, cualquier cosa que el puntero pueda gestionar, es la misma gente que por otro lado repudia el aparato, lo denosta, pero a la vez le tributa. Todo esto es una relación sumamente compleja.

El voto electrónico, supuestamente, viene a ser la negativa de este sistema de dominación. Es como la reasunción de una cierta autonomía individual en un sistema en el que se piensa que la política degrada, ensucia, es turbia porque pacta con el punteraje. Ahí aparece el

imaginario del voto electrónico como salvador, la máquina y yo definimos un nuevo acuerdo que hace que la política se vea limpia. Esa es la razón, a mi modo de ver, por la que se permea el discurso del voto electrónico con tanta facilidad, incluso en partidos y políticos progres, o seudo progres (o lo que eso signifique hoy día). Acríticamente se compra el discurso del voto electrónico.

BB: Lo que sorprende es que no se discute, al menos desde esos ámbitos seudoprogres, la idea de la privatización del acto de votar, la privatización de un acto fundante de la democracia y la política.

MH: Por supuesto que no, aquí nadie habla de la composición accionaria de las empresas que proveen estas 'soluciones'. La separación del universo conceptual de política y empresas, sea en regulaciones tanto como en el discernimiento de quiénes son efectivamente los dueños del capital, forma parte del vaciamiento de la política.

Este tema se da de manera fenomenal. Hoy día se exige a cualquiera que hace campaña política, que diga de dónde saca cada centavo. Pero si se hace una campaña por voto electrónico como contrapartida a la lista sábana, nadie pregunta de dónde se obtiene el dinero. Una cosa que es fundamental en este proceso, es que en caso de que se realicen estas pruebas piloto de las que tanto se habla, es indispensable saber quién las paga, de dónde vienen los fondos para hacer esas pruebas, porque se corre el riesgo de que eso se termine pagando como campaña de bien público sin que se pida cuentas a quien está usando los medios de comunicación y la estructura del estado para torcer la opinión pública.

En este tema, no existe auditoría de quién y cómo se paga la campaña. El sistema de cooptación empieza desde los funcionarios mismos que deciden, lo cual es un tema muy complejo. Veamos por caso, si vos sos un funcionario del Ministerio del Interior y te invita el Tribunal Superior de un país latinoamericano, por ejemplo Nicaragua, a ver sus elecciones, eso es una cosa. Ahora, si el que te invita es un consorcio de empresas que tienen la concesión del voto en Nicaragua para que vayas a ver cómo funciona su sistema, eso es otra muy diferente, porque ahí lo que vas a ver no es cómo funciona el sistema, sino su sistema y su servicio.

Una cosa es si la invitación viene del gobierno y otra es si viene de la empresa proveedora del sistema. Sabemos que la acumulación de portafolios, como se suele decir a la asistencia regular a congresos y eventos, no es menor a la hora de tomar decisiones políticas.

BB: ¿Qué rol juega el mundo académico argentino en esta discusión hoy día. Sabemos que en los EEUU, las Universidades como Princeton o la de California son las más críticas de estos sistemas y que tienen un rol firme en dar las alertas públicas. ¿Con qué nos encontramos aquí?

MH: Nosotros hemos habilitado la discusión para que el sector académico participe del debate. De hecho, invitamos a la Universidad de Cuyo a la jornada del 30 de Mayo pasado. Pero más allá de eso, y más allá de alguna intervención de investigadores del Instituto Gino Germani (de Ciencias Sociales de la UBA) o de Ciencia y Técnica, no hay demasiado debate. Hubo algunos artículos que generaron una seguidilla de discusiones, pero eran de tipo más bien periodísticas, sólo ilustrativas, nada demasiado profundo. Para nosotros es importante incentivar al mundo académico para que participe de esta discusión.

BB: Imaginando un escenario donde se apruebe la normativa y se instale el voto electrónico, ¿qué nos queda por hacer a los ciudadanos que pensamos que esto es malo para nuestra democracia y queremos detenerlo?

MH: Las leyes electorales por lo general requieren mayorías especiales, según está consagrado en nuestra Constitución de la ciudad. Una ley de este tipo, para ser aprobada e implementada, requiere un acuerdo previo muy fuerte, ya que lo que está en juego son las propias reglas de juego del sistema político. Una vez que se logra un acuerdo fuerte de tal naturaleza, es muy difícil revertirlo.

Un recurso de amparo ciudadano, en un caso así, no tendría demasiado futuro, ya que iría contra un acuerdo político ciertamente sólido. Sólo en caso de que haya un verdadero desastre, que se pruebe la falencia absoluta del sistema y que se produzca un escándalo mayúsculo se podría revertir una situación así.

BB: Como lo ocurrido en Las Grutas en diciembre de 2007, donde la gente presentó un amparo que fue desoído por la justicia, pero el día de las elecciones la implementación fue tan escandalosa que el Concejo Deliberante finalmente derogó la ordenanza que habilitaba el uso de voto electrónico.

MH: Exacto, salvo en un caso de ese tipo, es muy difícil dar vuelta un consenso basado en un acuerdo político de este tipo. Si no se verifica efectivamente un daño a la voluntad popular, es muy complejo revertir una cosa así.

Buenos Aires no es Las Grutas, en términos de magnitud del distrito. Si se implementa, tendría que haber un fallo brutal y un estado de conciencia donde la mayoría inicial que dio base al acuerdo se diluyese. En tanto no se diluya en el sentido común, es muy difícil que alguien asuma públicamente que el régimen que acaba de aprobar es una porquería.

BB: Como lo que pasa en Brasil, donde los expertos en seguridad informática tienen prácticamente censurada toda opinión que pueda poner en duda la fiabilidad del sistema electoral.

MH: Así es, pero además pensemos en otro eje importante de la discusión. Para deslegitimar el voto manual y el sistema de partidos políticos, en Argentina, se vienen usando picardías de todo tipo desde el retorno a la democracia en el 83.

Siempre se ha tratado de hacer trampa. En el plebiscito sobre el archipiélago del Beagle la actual Ministra de Defensa Nilda Garré intentó votar en cuatro mesas diferentes porque tenía dos documentos y le fue mal, creo que hasta terminó procesada, fue una calamidad. Siempre se ha tratado de hacer trampa y, aún así, la gente sigue creyendo en los sistemas electorales. Por eso es que todo el material de esclarecimiento sobre esto hay que usarlo y difundirlo ahora, antes de que se implemente. En la conciencia de la gente, las elecciones en los EEUU, aquella donde George W. Bush derrota a Al Gore dejan la percepción de que hubo algo sucio. Este tipo de casos sirven mucho más que el razonamiento tecnológico para que la gente lo entienda.

El sistema electoral es como la virtud de la novia, vos la podés discutir hasta el día que se casa, seguir discutiendo al día siguiente sólo hace daño porque hay que santificar el matrimonio. Esto funciona igual, una vez que se impuso, ya es tarde para hablar. Son acuerdos tan profundos, que movilizan tantas voluntades, votos legislativos, relaciones de dominación, pactos, acuerdos, que cuando querés salir a advertirlo una vez consensuado la cosa se complica mucho más.

BB: Y ni hablar de los negocios que esto moviliza.

MH: Hoy día, hay otro tema que es imprescindible discutir, que tiene que ver con los fondos de campaña. En mis 36 años de militancia política he visto de todo. Viví todas las formas de ingeniería social. En los 70s, si tenías un imprentero amigo, ese era tu jefe de campaña, porque su

aporte era en volantes, panfletos, carteles. Hoy día, todo eso está diluido en el cash, el efectivo.

Hoy día, las campañas se manejan única y exclusivamente con dinero en efectivo. Ya no se trata de reunir recursos, hoy todo pasa por el efectivo. Y ahí es donde está la parte crucial, en la relación de los candidatos con las empresas que financian sus campañas y en este sistema de maridaje especial entre empresas, corporaciones y políticos. Ahí es donde está la plata, ahí es donde se resuelven las campañas. Y ahí es donde hay que empezar a indagar si queremos transparentar los procesos políticos.

BB: En EEUU, de las tres grandes empresas que proveen urnas electrónicas, dos tienen probados vínculos con el partido republicano. Una de ellas(ES&S) de hecho, tiene a un senador republicano entre sus principales accionistas.

MH: Eso es un ejemplo más que elocuente de este maridaje de empresas y política.

Notas

1- http://votobit.southtechnologies.com.ar/

Debates legislativos en la Ciudad de Buenos Aires

Compilación a cargo de Beatriz Busaniche

El 30 de mayo de 2008, gracias a la coordinación del Bloque Igualdad Social, la legislatura de la Ciudad de Buenos Aires abrió sus puertas a un debate que a todas luces es indispensable. El título de la jornada hizo énfasis en "Transparencia y métodos de votación"[1] como ejes para conversar entre diferentes actores políticos sobre la necesidad de mejorar el sistema político de la ciudad y las herramientas que se evalúan para tal fin, entre ellas, el voto electrónico y la boleta única.

La presentación, por parte del legislador del Partido PRO (Macrismo) Cristian Ritondo, de un proyecto de uso e implementación de voto electrónico en la Ciudad de Buenos Aires fue la excusa perfecta para abrir un debate del que participaron expertos de organizaciones sociales y cuatro legisladores en representación de diferentes bancadas políticas de la ciudad.

La ciudad de Buenos Aires adolesce todavía de algunas leyes que le hacen falta para consolidar su sistema politico. Carece aún de una ley de partidos políticos, de financiamiento de la política y de un código electoral propio. Es en este marco que se dan hoy día las discusiones sobre la incorporación de sistemas electrónicos de emisión de voto, en las que no queda claro todavía cuál es el problema que se pretende solucionar con la incorporación de estos sistemas.

En su intervención de la jornada del 30 de mayo, la Diputada del Frente para la Victoria, Silvia La Ruffa, fue clara al decir que "cuando ponderamos las virtudes o los fundamentos del voto electrónico o de la boleta única, nos encontramos con discursos que van en contra de la solución de aquellos problemas que son centrales en la relación representante–representado. Se construye la necesidad del

empoderamiento de la sociedad civil sobre la base de la debilidad de las instituciones políticas, tanto de los poderes constituidos como de los partidos políticos." Así, La Ruffa trae al debate un tema central, que tiene que ver con la relación representado-representante en el marco de la acción política.

"Aunque los partidos políticos hayan dejado mucho que desear en su accionar del ´83 a la fecha, la verdad es que no hay régimen democrático estable que no se estructure sobre la base de un sistema de partidos políticos, más o menos fragmentado, bipartidista o con cinco o seis actores. Existe un argumento central en el discurso de aquellos que promueven la implementación del voto electrónico, que enfatiza que son necesarios menos fiscales. Siguiendo esa línea argumental, se les quita a los candidatos, a los partidos políticos, a las alianzas electorales el desafío de que su base de sustentación requiera una estructura que le permita en el momento eleccionario garantizar el control en la elección. De esta manera, se promueve la fragmentación de la oferta electoral, que conlleva a una menor capacidad social para agregar representaciones" agregó La Ruffa.

"Cualquier herramienta electoral que se implemente en el futuro no debe ser evaluada de manera aislada. Sin duda, su promoción va acompañada de intereses, independientemente de las virtudes o defectos inherentes a las mismas. El desafío consiste en desarmar ciertos mitos que se generan en torno a la emisión electrónica del voto de manera tal que se promueva la generación de espacios de reflexión en los cuales, aunque en las decisiones intervengan variables políticas, sean tenidas en cuenta las recomendaciones y sugerencias de los expertos en la materia" expresó la legisladora del Frente para la Victoria como corolario a su intervención en la cual el énfasis estuvo dado por la importancia de la participación ciudadana y el fortalecimiento de los partidos políticos como eje de la política de representación democrática.

A su turno, y en esta misma línea, el representante de la Coalición Cívica, Sergio Abrevaya, fortaleció los conceptos relacionados con la participación ciudadana, al decir que:

"En las comunidades donde los ciudadanos se involucran activamente en el control, sea a través de la presencia de fiscales o porque los presidentes de mesa se encuentran informados y tienen un rol relevante durante el comicio, los mecanismos se tornan más transparentes ya que es la comunidad quien controla. Eso facilita la discusión acerca de los elementos de votación actuales y permitiría introducir en el debate la implementación del sistema de voto electrónico. Incluso cuando cualquier propuesta electrónica

presenta problemas, porque lo informático es vulnerable, es la comunidad quien observa lo que está sucediendo durante la emisión de voto."

Estos comentarios de Abrevaya plantean de manera tangencial un tema central: el control ciudadano sobre el acto de emisión del voto y la pérdida de capacidad por parte de las personas comunes sin conocimientos de informática de la potestad de controlar y auditar el proceso mientras participan de él.

"La transparencia sólo es posible en la medida que la sociedad se involucre" agregó Abrevaya*, "la responsabilidad de que esto ocurra es, en parte, del Estado. Sin embargo, la comunidad debe articular su demanda de mayor transparencia. En la medida en que la comunidad no esté involucrada no va a haber ningún sistema que tenga capacidad de modificar esta realidad".*

Esta afirmación, si bien no directamente relacionada al voto electrónico, nos remite a la necesidad de participación ciudadana para la construcción de la confianza y la transparencia de proceso y nos obliga a preguntarnos en qué medida la incorporación de una caja negra de difícil comprensión por parte de buena parte de la ciudadanía puede aportar positivamente a ese proceso.

Cristian Ritondo, impulsor de la incorporación de voto electrónico para la ciudad, tomó la palabra tras la presentación de Abrevaya y subrayó que:

"el voto electrónico es un proceso de largo alcance ya que, más allá de la confiabilidad de cualquiera de los sistemas, no es posible implementar dicho instrumento de una elección a otra. Creo que la boleta única salda algunos problemas y que su implementación no atenta contra la presencia de fiscales. En Argentina después del proceso del 2001 ha quedado claro que hay muchos partidos que tienen fuerte presencia en algunos distritos pero no en otros. En la Provincia de Buenos Aires se presentaría como un grave problema la ausencia de fiscales ya que las mayores dificultades de provisión de boletas proviene de ese distrito. Este es uno de los problemas que podrían saldase en el corto plazo a través de la implementación de la boleta única. El sistema de voto electrónico no excluye ni contradice a la boleta única."

"Por otra parte", continúa diciendo Ritondo, *"se presenta como un tema a tratar el sistema de voto electrónico. En el sexto encuentro de Votobit pudimos constatar que existe un cierto fanatismo por parte de aquellos que creen que es la panacea y, por otro lado, hay*

personas que plantean que el voto electrónico no sirve para nada. Sin embargo, yo creo que hay un camino intermedio que implica que hay que aprender de las experiencias, hay algunas que han salido mal y otras que han salido bien. No sólo debemos tener en cuenta las experiencias exitosas, creo que hay que incorporar, además, aquellas cuestiones que tienen que ver con la idiosincrasia y hábitos electorales de los argentinos. Pensando en esta clave, en el proyecto que hemos presentado en la Legislatura decimos que debe haber un respaldo físico, ya que el elector argentino tiene como costumbre ver lo que vota, inclusive hay sistemas que imprimen la boleta y la depositan en una urna. Como garantía, considero que es la mejor, al menos hasta que cualquier sistema y cualquier modificación de sistema tenga la confianza de la gente, lo que supone que aquel que emita su voto en forma electrónica esté seguro que la máquina cuenta los votos correctamente. Este tema puede ser comparado con los cajeros automáticos que, cuando aparecieron en el país trajeron muchas dudas. Sin embargo, los usuarios vieron aumentar su nivel de confianza con el uso habitual a lo largo del tiempo y, actualmente, muchos pagan sus servicios y utilizan el cajero cotidianamente sin desconfiar de él. Considero que vamos en camino hacia el voto electrónico, soy un impulsor del mismo, si bien con ciertos recaudos."

"Existe un alto nivel de consenso respecto de la necesidad de una ley electoral y una ley de financiamiento de los partidos políticos en la Ciudad de Buenos Aires y sobre ello hay que ponerse a trabajar. La presencia de los partidos, independientemente del sistema de votación que se implemente, es fundamental. En el caso del voto electrónico, las exigencias a los partidos tienen características particulares, ya que deben participar del proceso electoral contando con fiscales formados en temas informáticos. Por otra parte, durante el acto electoral sigue habiendo un problema ya que si bien la urna es electrónica, son personas las que exhiben el documento y quienes chequean la identidad del elector en el padrón. Esto indica que la cantidad de electores y la presencia física seguirán siendo importantes" explicó el Legislador macrista a la hora de defender el proyecto que impulsa. Para luego rematar su intervención diciendo que *"el voto electrónico es una herramienta que contribuirá a las modificaciones que queremos hacer para el cambio en la Ciudad de Buenos Aires."*

Notas

1- Fuente: Transparencia y Métodos de Votación. Bloque Igualdad Social. Legislatura de la Ciudad de Buenos Aires. Publicación de la Dirección General de Impresiones y Ediciones. Ciudad de Buenos Aires. Argentina. Esta publicación se distribuye bajo una licencia Creative Commons, By, No realizar usos comerciales. Ver http://creativecommons.org/licenses/by-nc/2.5/ar/

ensayos



La certeza de la incertidumbre: lo que no se dice sobre el Voto Electrónico

Alfredo Daniel Rezinovsky

Facultad de Ingeniería

Universidad Nacional de Cuyo*

En general en los eventos sobre voto electrónico, sobre cuestiones legales opinan abogados, sobre política politólogos y sobre la parte técnica opinan vendedores de equipos de voto electrónico. Me sorprende muy gratamente que se me haya invitado a exponer como especialista independiente.

Quienes apoyan los sistemas de voto electrónico pregonan numerosas ventajas que nunca llegan a demostrar en forma sólida, ni en teoría, ni mucho menos en la práctica.

La principal ventaja que se atribuye al voto electrónico es la transparencia. Un equipo de voto electrónico es básicamente una computadora, con sistema de entradas y salidas, un sistema operativo y software. Para poder garantizar qué es exactamente lo que está haciendo una urna electrónica hay que ser especialista en sistemas de información, programación, compiladores, sistemas operativos y microelectrónica, además de tener las

herramientas que permitan examinar los dispositivos a fondo. Hay pocos equipos de especialistas capaces de reunir estos conocimientos y ciertamente ningún individuo por sí mismo puede asegurar qué está pasando en una urna electrónica. La urna electrónica es una caja negra que de ninguna manera puede agregar transparencia a los procesos.

La dificultad para analizar las urnas hace que tengan que verificarse por muestreo, después de lo cual son almacenadas, transportadas y manipuladas por muchas personas hasta llegar a los lugares de votación. En ese momento sólo podemos confiar ciegamente en que todo está bien, no hay posibilidad de verificar nada más.

La segunda ventaja que nos quieren vender es la seguridad y la confiabilidad. Las computadoras fallan y son vulnerables, todos lo sabemos. Sistemas hechos por empresas con 30 años de experiencia en sistemas operativos fallan y son vulnerados pocos días después de salir a la venta. Incluso en sistemas de código abierto se descubren a veces fallas que llevan años en los programas. El atractivo de atacar un sistema de voto electrónico hace además que las medidas de seguridad a las que estamos acostumbrados sean obsoletas. La teoría de control de calidad de software explica que sólo podemos garantizar que hay fallas si las encontramos, pero no podemos garantizar la ausencia de las mismas al no encontrarlas. Si en lugar de fallas se trata de vulnerabilidades intencionales encontrarlas se hace aún más difícil.

Recientemente se han detectado fallas en sistemas de voto electrónico usados en EEUU por las cuales algunos votos "desaparecían" al trasladar los datos. Esas fallas estuvieron ahí durante más de 10 años y nadie las vio. Y lo que es peor aún, nunca vamos a saber cuántos ni cuáles votos se perdieron en elecciones reales usando esos equipos.

De lo que se habla poco es de la privacidad y el secreto de voto. No creo que nadie se anime a revelarle a otro el voto para que lo anote y lo contabilice. Sin embargo, a casi nadie le molestaría dar su voto a una máquina de la cual no sabe absolutamente nada. Se debe suponer, sin pruebas ciertas, que no se está grabando o transmitiendo ninguna relación entre el voto y el votante. Con el voto electrónico se elimina el voto cadena. Pero el voto cadena es sólo una forma eficaz de violar el secreto de voto para poder torcer la voluntad del votante. Con voto electrónico el secreto de voto podría violarse de forma eficaz y además eficiente como ha ocurrido en algunos casos concretos, por ejemplo, en Ohio (EEUU) o en Holanda.

¿Se puede hacer sistemas de voto electrónicos seguros? Probablemente sí. ¿Puede alguien verificar que lo son? No. Esa incertidumbre hace que se pierda completamente el control por parte del votante, por parte de los auditores y por parte de los técnicos. Las autoridades

de mesa se convierten en meros espectadores del proceso, y únicamente quienes fabricaron el sistema de voto electrónico y quienes lo han manipulado tienen control sobre la elección y sobre los resultados.

* Este artículo es una desgrabación de la ponencia de Alfredo Daniel Rezinovsky realizada el 30 de mayo de 2008 en la ciudad de Buenos Aires. Salón Montevideo. Legislatura de la Ciudad de Buenos Aires.

"Lo que cuenta no es el voto, sino quién cuenta los votos"*

Beatriz Busaniche

Pasada la última elección para Jefe de Gobierno de la Ciudad de Buenos Aires y con la victoria de Mauricio Macri, se ha hecho recurrente escuchar en medios de comunicación masivos una prédica en favor de la implementación de sistemas de voto electrónico en las distintas circunscripciones electorales. Así, a pocas horas de conocido el resultado de la primera vuelta en Capital, partidarios de este sistema salieron a los medios a decir que "es irrisorio esperar tres horas por los resultados de una elección y que es urgente la implementación de voto electrónico". Lo mismo ocurrió durante la jornada electoral de la segunda vuelta.

La pregunta que nos debemos hacer frente a estos actos de propaganda es ¿El voto electrónico mejora la democracia?

En este escenario, recordamos que es unánime el rechazo de los expertos en seguridad informática a los sistemas de votación mediados por computadora, y que son conocidas las experiencias en las que estos sistemas se han mostrado no sólo fallidos, sino altamente permeables al fraude electoral.

El voto es el acto fundamental de la democracia, y por tanto, no se lo puede arriesgar a manos de un discurso basado en la fantasía de la existencia de soluciones técnicas para problemas políticos y que no ofrece ninguna

comprobación eficiente de las virtudes que pregona.

Se escucha decir, en forma recurrente, que los sistemas de votación electrónica:

1. Ofrecen mayores facilidades al elector para el ejercicio del derecho al sufragio;
2. Fortalecen la transparencia de los procesos electorales;
3. Disminuyen las posibilidades de fraude;
4. Aceleran el proceso de obtención de resultados del escrutinio;
5. Simplifican el sistema de voto y escrutinio;
6. Disminuyen la abstención de votos;
7. Reducen los costos, al evitar el escrutinio provisorio.

Salvo el postulado sobre la rapidez en la obtención de resultados, ninguna de las demás afirmaciones tiene asidero en la realidad. Más bien todo lo contrario.

De hecho, los sistemas de votación electrónica no sólo no disminuyen las posibilidades de fraude, sino que lo simplifican y tornan más económico, al centralizar su posible implementación. La cuestión de la transparencia no es un tema menor. **La implementación de voto electrónico reduce considerablemente la cantidad real de personas capacitadas para auditar una elección**. Hoy día, el sistema educativo básico garantizado por ley otorga a la ciudadanía los conocimientos mínimos indispensables para ejercer su derecho constitucional a auditar una elección como fiscal de un partido. Para esto, en el modelo actual sólo hace falta saber leer, contar y escribir y tener el compromiso para participar activamente. Implementando cualquier sistema de votación electrónica, estos conocimientos mínimos se elevan de tal forma que sólo una ínfima fracción de la sociedad estará en condiciones de ejercer ese derecho que es de toda la ciudadanía. ¿Estamos dispuestos a renunciar a un derecho constitucional así como así?

Hará falta ser experto en software, hardware y en auditoría de este tipo de sistemas para conformar una corte de auditores privilegiados en manos de quienes quedará el destino de nuestras democracias. Esto, sin contar los casos en los que los programas han sido deliberadamente escritos para ser inauditables (programas con millones de líneas de código como es el caso de Brasil) o en los cuales hay secciones completas que no se someten a escrutinio público. Ocurre otro tanto en el caso de que el software o el hardware que fue auditado sean diferentes de los usados en cada circunscripción. ¿Quién garantizará efectivamente que

el programa auditado por los denominados fiscales informáticos es el que está corriendo en cada una de las miles máquinas de votación? ¿Quién asegurará que ese mismo hardware no haya sido adulterado? Recordemos que existe probada evidencia de que adulterar una máquina de votación no demanda conocimientos demasiado complejos y es una operación que se puede realizar en cuestión de minutos.

Otra promocionada ventaja indica que los partidos minoritarios no necesitarán reunir un gran número de fiscales para tener representación equitativa en las mesas electorales. La pregunta es, si esos mismos partidos tendrán la capacidad de contratar suficientes auditores informáticos para cubrir las necesidades impuestas por el novedoso sistema.

Mucho se puede hablar también de la supuesta facilidad para los electores y la reducción en la abstención. ¿Qué tipo de interfaz se debe desarrollar para garantizar la posibilidad de votar en un sistema donde hay una enorme cantidad de candidatos y donde se vota por varios cargos de diferentes niveles a la vez?

Por otro lado, vale mencionar que la creciente abstención de votantes es un problema social y político que no tiene solución a la vista en el campo de la informática.

Sin dudas, el otro gran elemento de propaganda es la supuesta economía que implica la votación electrónica. Esta es otra probada falsedad. En países como Bélgica está comprobado que los sistemas de votación electrónica son tres veces más caros que los de votación tradicional con sistema de papeletas. Este dato es fácilmente corroborable si multiplicamos el costo de poner una terminal de votación en cada una de las circunscripciones electorales del país o lo que costarán los servicios de auditores profesionales.

Es unánime la crítica a estos sistemas por parte de los especialistas en sistemas de seguridad informática. No hay forma de garantizar la transparencia en una elección mediada por computadoras y mucho menos sin invertir una cuantiosa suma de dinero en mecanismos de validación que darían por tierra con las mentadas ventajas de tiempo y costos que tanto se promocionan.

Todo esto con el objetivo de reducir en unas pocas horas la obtención de un resultado de una elección que se realiza con intervalos de varios años. Lo que se pone en el lado de los supuestos beneficios pierde peso cuando se balancea con los peligros que trae una "solución" de este tipo. Los riesgos de una implementación de mecanismos de votación electrónica son demasiado altos como para justificarlos en el ahorro de unas pocas horas.

Las posibilidades de fraude se simplifican de una manera sorprendente mientras que los costos a pagar por un cambio de esta naturaleza son lo suficientemente altos

como para aventurarse en una experiencia de "e-votación" sin el mínimo escrutinio público y discusión con todos los sectores interesados.

Ni siquiera el uso de Software Libre es condición suficiente para una implementación confiable de votación electrónica.

Cambiar nuestro actual sistema electoral por mecanismos de esta naturaleza, sin escuchar las advertencias de los expertos y sin la necesaria discusión e información pública, no será una mejora para nuestra democracia, sino un paso irremediable hacia una tecnocracia que poco tendrá que ver con la constitución de una República comprometida con los valores de la participación, la democracia y los derechos ciudadanos.

Notas

* La frase que da título a este artículo se atribuye a Josef Stalin

¿El voto electrónico mejora la democracia?

Federico Heinz

El llamado “voto electrónico” está siendo promovido como una alternativa eficiente y segura para la emisión del sufragio. La afirmación de que es seguro, sin embargo, choca con las conclusiones de la comunidad científica, que afirma que no es posible construir una urna electrónica segura. La votación es un elemento demasiado central a nuestra forma de vida como para basarlo en mecanismos no controlables.

Eficiencia vs. Eficacia

En los últimos tiempos, se escuchan voces promoviendo el voto electrónico y destacando lo que perciben como sus ventajas. Algunas de estas voces llegan a pintar a los dispositivos de voto electrónico como la cura a muchos de los males de la democracia moderna. En algunos países, el voto electrónico ya es usado ampliamente, y en los demás se realizan pruebas piloto, conferencias y eventos para promover su uso. Los argumentos a favor de esta modalidad de votación generalmente destacan que las urnas electrónicas impiden ciertos tipos de fraude electoral, por ejemplo el voto en cadena, y que las urnas electrónicas permiten hacer elecciones más eficientes: no es necesario

imprimir boletas, con lo que se reducen costos, y los resultados pueden ser anunciados con mayor rapidez, ya que el escrutinio es automático. Esto permitiría, incluso, reducir tanto el costo de las votaciones que volvería económicamente factible votar con más frecuencia, y sobre más cosas, lo que permitiría una mejora de la calidad de la democracia.

Dejando de lado por un momento que la sociología y las ciencias políticas nos enseñan que más elecciones no equivalen a más democracia, el argumento de la eficiencia es muy seductor en nuestros tiempos. Tan seductor que, sin darnos cuenta, a menudo sacrificamos eficacia (es decir, hacer bien las cosas necesarias) a cambio de eficiencia. En las sabias palabras de un gran amigo, “nada hay peor que hacer eficientemente lo que uno no debió hacer nunca.” El ejercicio del sufragio es esencial a nuestro modo de gobierno. Es mucho más importante hacerlo bien que hacerlo rápido o barato.

OTRAS ALTERNATIVAS EFICIENTES

Si efectivamente lo que nos ocupa es la eficiencia de la emisión y conteo de votos, me tomaré la libertad de proponer una alternativa de mi invención, que presenta todas las ventajas de las urnas electrónicas y agrega algunas propias: el voto eclesiástico. La idea es muy sencilla: en vez de convocar a los ciuadadanos a que voten en las escuelas, podemos pedirles que vayan a las iglesias a votar. En ellas, los fiscales de los partidos verificarán sus documentos, y dirigirán al elector a un confesionario. Una vez en el confesionario, el ciudadano le comunica al sacerdote su voto, y éste lleva la cuenta haciendo anotaciones en un cuaderno. Cerrado el acto eleccionario, los sacerdotes de la parroquia se reúnen, comparan notas, y anuncian el resultado local, comunicándolo a la diócesis. Ésta consolida los resultados de las parroquias, los anuncia y comunica a la arquidiócesis, y así hasta llegar al Obispado, que finalmente anuncia el resultado definitivo.

El procedimiento es sencillo y eficiente, utiliza infraestructura existente, tiene bajos costos, elimina algunas formas de fraude, y puede proporcionar los resultados con una rapidez comparable a la del voto electrónico. Además, tiene la enorme ventaja de que involucra, como garantía del proceso, a una institución que predica la verdad y el amor como virtudes supremas, y cuyos agentes han jurado dedicar su vida por entero a esos ideales.

Sin embargo, cualquier persona de vocación democrática, independientemente de si profesa la fe

católica o no, sabe que lo que acabo de proponer es un disparate inaceptable. La razón es muy sencilla: además de confianza, necesitamos control. Por mucho que confiemos en la Iglesia como institución, nadie aceptaría un escrutinio hecho de la manera descripta más arriba porque no es posible controlar que nadie en el proceso haya falsificado los resultados.

Esto mismo se aplica al voto electrónico: dentro de las urnas electrónicas hay un programa que, al igual que el sacerdote dentro del confesionario, lleva la cuenta de los votos haciendo notas internas. Cualquier persona que conozca los rudimentos de la programación de computadoras sabe lo sencillo que es hacer un programa que mienta sobre los resultados de una elección. Los especialistas en seguridad informática de todo el mundo advierten en numerosas publicaciones que es matemáticamente imposible hacer un sistema de voto electrónico puro en cuyos resultados se pueda confiar. Las mismas urnas electrónicas que vuelven imprácticas algunas formas actuales de fraude electoral, abren la puerta a una nueva forma de fraude, una que permite la falsificación masiva y a muy bajo precio de los resultados.

Mecanismos de control

Existen varias alternativas de control para las urnas electrónicas. Lamentablemente, casi todas ellas presentan el problema de que, al usarlas, las ventajas del voto electrónico desaparecen.

El mecanismo de auditar completamente el funcionamiento de las urnas es impracticable. Esta es una tarea que sólo podría ser ejecutada por una élite de especialistas, de los que hay muy pocos en el mundo, y requiere la cooperación de las empresas que proveen las urnas así como de todos sus proveedores. Y aún si consiguiéramos todo eso, la eficacia de una auditoría sería más que dudosa: no sólo debemos garantizar que todo el software es correcto (lo que es imposible), sino que además debemos verificar que el software presente en las urnas el día de la elección es idéntico al auditado, tarea que nuevamente requiere de especialistas. ¿Y por qué hemos de confiar en los especialistas, si no queremos confiar en sacerdotes ni en empresas? Una de las muchas virtudes del "anticuado" sistema de escrutino tradicional es que cualquier persona que sepa leer, escribir y hacer operaciones de aritmética elemental está en condiciones de controlarlo. Esta es una característica esencial y no debemos renunciar a ella.

Existen mecanismos criptográficos muy ingeniosos, que permiten que cualquier ciudadano mínimamente entrenado pueda controlar que su voto ha sido contabilizado correctamente. Este es un nivel de control mayor incluso que el que es posible usando el sistema tradicional. Lamentablemente, tienen el problema de requerir equipamiento e insumos especiales, que aumentan el costo hasta hacerlo más caro que la alternativa analógica, y además vuelven a introducir la posibilidad de fraude: si el elector puede verificar que su voto fue contado correctamente, también puede usar esa información para demostrar ante terceros que votó de una cierta manera, lo que facilita la compra de votos.

La única posibilidad razonablemente verificable de usar voto electrónico sin tirar por la borda la seguridad electoral es mediante urnas que lleven un registro físico en papel de los votos emitidos. Lamentablemente, esto es caro, y más difícil de lo que parece: cualquier persona que haya tratado de descifrar un ticket de supermercado puede imaginar la pesadilla que podría ser desentrañar una boleta electoral impresa en formato ticket, y además queda por resolver qué hay que hacer con los tickets para que sea posible contarlos para contrastar con los totales de la urna y al mismo tiempo sean inútiles como comprobantes de haber votado de cierta manera.

Una alternativa factible es realizar la votación mediante formularios que contengan a todos los partidos, dejar que los votantes marquen su elección con tinta, y usar un scanner óptico para hacer un escrutinio automático, verificable mediante un simple recuento manual. No hay nada en contra de un escrutinio electrónico, pero digitalizar el acto mismo de la emisión del voto es extremadamente peligroso para la democracia.

Privatizar el voto

Patricio Lorente*

El 28 de octubre de 2007 hubo elecciones nacionales. En casi todos los centros urbanos, pero especialmente en la zonas urbanas más pobladas de Capital Federal y las provincias de Buenos Aires, Córdoba y Santa Fe, las colas de ciudadanos esperando su turno para votar se pudieron ver hasta las nueve de la noche, e incluso más tarde, prolongando en más de tres horas el horario de cierre de los comicios.

El malestar de los electores que debieron ejercitar su paciencia durante varias horas para poder emitir su voto, el caos de los cuartos oscuros presentando varias decenas de distintas ofertas electorales, la confusión que generaba la existencia de listas distintas pero con idénticos candidatos para algunas categorías, el cansancio creciente de las autoridades de mesa y fiscales, hicieron de esas elecciones quizás las más desprolijas desde el retorno a la democracia en 1983, pero no las únicas con esa característica: los comicios ya venían siendo crecientemente lentos y desordenados.

Al día siguiente, entre resultados parciales y análisis políticos, muchas voces se alzaron para reclamar la implementación del voto electrónico. No era un reclamo novedoso, pero cobraba particular fuerza por el fastidio de una jornada bochornosa, cuya culpa aparente -según algunos, evidente- se podía encontrar en la reticencia de los dirigentes locales en modernizar la tecnología mediante la cual se emiten y se cuentan los votos.

Sólo en un medio, el diario La Nación, al menos dos columnistas más la nota editorial del día abogaron por reemplazar las urnas tradicionales por máquinas electrónicas. Joaquín Morales Solá tuvo un párrafo lapidario dedicado al Ministro del Interior: “Fue, todo hay que

decirlo, la elección peor organizada desde 1983. El ministro del Interior, Aníbal Fernández, comenzó su gestión con la promesa del voto electrónico inmediato, y se va, más de cuatro años después, dejando los comicios más desprolijos de la democracia. La política argentina tiene una rara vocación para convertir en tortura ciudadana hasta lo que debió haber sido un acto de alegría cívica"[1]. Fernando Laborda envidió a los vecinos brasileños: "Nuestra logística electoral se mostró ayer parcialmente incapaz de canalizar en orden el voto ciudadano y contrastó con la practicidad que en países vecinos, como Brasil, posibilita el voto electrónico, una alternativa que, desde hoy, deberá comenzar a considerarse aquí"[2]. La editorial destacaba un debut que en realidad no fue tal: "Por último, en la ciudad fueguina de Ushuaia, donde se inauguró con éxito el voto electrónico, se reeligió como intendente al dirigente del Movimiento Popular Fueguino Jorge Garramuño, quien aventajó al postulante del justicialismo"[3].

Se trata sólo de una muestra: la misma demanda se multiplicó en distintos medios y por distintas voces, incluyendo dirigentes políticos de distintas pertenencias partidarias e ideológicas. El reclamo caracterizaba de manera general al voto electrónico con los atributos de agilidad y transparencia, aunque no hubo quien se molestara en explicar de qué manera se agilizan y se transparentan los comicios mediante esa innovación.

Curiosamente, nadie señaló que al menos en los últimos dos comicios nacionales las mesas de votación han sufrido una silenciosa inflación: de 290 electores que votaba en cada mesa desde 1983 se ha pasado a 390. Si las mesas abrieran puntuales, cada elector tendría un promedio de un minuto y medio para completar el trámite de votación para que la mesa terminara su labor a las 18.00 horas. Cierto es que nunca votan todos los electores, pero el porcentaje de votantes sigue siendo asombrosa y felizmente alto. Y además es menester agregar pausas para que los fiscales controlen el cuarto oscuro y ya es de rutina que existan demoras en la apertura de las mesas provocadas por la tardanza en la llegada de las urnas y/o del personal de custodia.

En esas condiciones, no parece ser la tecnología de votación la causa principal de las demoras. Y al respecto, resulta aún más curioso que la referencia al uso de urnas electrónicas en Ushuaia no incluyera que las demoras en ese distrito se contaran entre las más exasperantes de la jornada pese a que se utilizó sólo para la elección del intendente municipal -es decir, un voto mucho menos complejo que el que debía emitir cualquier elector de la Provincia de Buenos Aires que incluía cinco categorías de candidatos y decenas de listas. Como es de esperar, a los problemas del siglo XIX -demoras en la entrega de las urnas, por ejemplo-, se le agregaron los propios del siglo XXI: cuelgues en las máquinas de votación, atascamiento de

las impresoras, etc. [4]. Esto no sólo sucede en lugares donde puede pensarse que la infraestructura no está preparada para incorporar estas innovaciones, sino que también pasa en cientos de circunscripciones de EEUU donde en la elección de 2004 se registraron colas aún más bochornosas que las de nuestra última elección o donde algunos jueces electorales ordenaron imprimir boletas para volver de urgencia al viejo sistema tradicional[5].

Es muy cierto que en elecciones complejas, el sistema de boletas de papel preimpresas para cada partido o coalición hace muy difícil hallar la opción de preferencia del elector. Al mismo tiempo, facilita prácticas nocivas que entorpecen aún más este proceso, como el truco de robar las boletas del partido rival o de esconderlas colocando sobre ellas boletas de terceros partidos.

Un sistema informático de emisión del voto permitiría prevenir la falta de boletas (aunque no es la única alternativa a este problema), más no la complejidad y consiguiente demora en la búsqueda de la opción de nuestra preferencia. Imagine el lector la siguiente situación: se encuentra frente a una pantalla donde se le muestran, sucesivamente un par de decenas de candidatos a Presidente de la Nación. Usted debe hallar su candidato, seleccionarlo, y confirmar esa selección. Luego debe encontrar su lista de candidatos a Diputado Nacional entre unas tres decenas de opciones y repetir el proceso. A continuación, debe hacer lo propio con el candidato a Gobernador. Luego, con los candidatos a legisladores provinciales. Más adelante, con candidatos a Intendentes. Seleccionadas todas sus opciones, debe confirmar (o corregir, lo que volvería el proceso al inicio). Y finalmente, emitir su voto. Parece ser mucho para un minuto y medio, teniendo en cuenta que una operación simple y de rutina en el cajero automático lleva algo más que ese tiempo.

En la provincia de Buenos Aires poco más de cincuenta mil vecinos emitieron su voto en urnas electrónicas. Según destacaron algunos medios, no se registraron inconvenientes ni largas colas, pero es menester señalar que se trató de mesas de electores extranjeros, que figuran en mesas de votación más reducidas que las comunes -por lo general, un tercio de electores- y que no se encuentran habilitados para votar cargos nacionales, por lo que se trata de un voto de menor complejidad.

La falta de boletas, por otro lado, puede solucionarse utilizando tecnología mucho menos compleja y más conocida: en lugar de boletas preimpresas por cada partido, puede implementarse un sistema de boleta única donde figuren las alternativas electorales y el ciudadano deba realizar una marca sobre la opción de su preferencia. Este mecanismo, que está previsto en distintos proyectos legislativos, facilitaría además el recuento de votos.

El reclamo de agilidad por parte de algunos medios incluye -y confunde- la rapidez en el trámite de emisión del voto, inquietud compartida por vastos sectores de la ciudadanía, con la velocidad en la determinación de resultados electorales. Esta inquietud tiene más fundamento en la ansiedad periodística que en la necesidad política del sistema democrático: salvo casos puntuales y excepcionales, los resultados se conocen a las pocas horas de terminado el comicio con aceptable precisión, si bien los datos definitivos demorarán algunos días (sin que esto afecte en nada la vida institucional). Tener ese dato a los pocos minutos o a las pocas horas carece de incidencia en la salud de la República.

Varios días de incertidumbre en la determinación del resultado final, máxime si se tratare de la elección de Presidente de la Nación, sí tendría consecuencias políticas e institucionales. El antecedente más cercano es la elección presidencial de los EEUU del año 2000, donde la elección entre George Bush y Al Gore se definió tres semanas después de haberse celebrado los comicios. No hubo, sin embargo, urnas y boletas tradicionales involucradas en el escándalo sino un moderno sistema semiautomático que incluía lectores ópticos y conteo automatizado.

Que la incorporación de tecnología agilice los comicios en cualquiera de estos casos parece ser más una expresión de deseos que una conclusión basada en hechos observables.

Lo mismo sucede con la mayor transparencia que, se supone, traerían consigo los sistema de voto electrónico.

Cuando las autoridades de una mesa de votación y los fiscales de los partidos políticos se aprestan a comenzar el comicio, realizan la operación -simple y confiable- de abrir la urna, verificar que se encuentre vacía y proceder a cerrarla y sellarla. En una urna electrónica, sea del tipo que sea, no existe el equivalente de esta operación. Bajo algunas condiciones teóricas[6] podría verificarse que la máquina está efectivamente en cero y que no realizará operaciones espúreas (como modificar los votos, por ejemplo), pero esta verificación requeriría de expertos y de equipamiento adicional cuya presencia en las 75.000 mesas de votación que habrá en la próxima elección nacional es fácticamente imposible. Y ello sin considerar que convierte al control ciudadano de las elecciones, piedra angular de la democracia, en una posibilidad reservada exclusivamente a un puñado de expertos.

A partir de escándalo de Florida en el año 2000, se han multiplicado los problemas con distintos tipos de urnas electrónicas y han existido informes de prestigiosas universidades demostrando, entre otras vulnerabilidades, la posibilidad de manipulación de los votos en distintos puntos del proceso y en ocasiones la posibilidad de identificar a los votantes y a sus respectivos votos[7]. Tal ha sido el

descrédito en los sistemas de voto electrónico que el Estado de California ha revocado la certificación de todas sus urnas electrónicas[8], pese a que en los últimos años ha invertido miles de millones de dólares en la adquisición de esta tecnología.

¿Por qué se supone entonces que es una opción más transparente? Revisando los argumentos de los defensores del voto electrónico se encuentra una sola explicación: la fe en la bondad de la tecnología; adicionalmente, la fe en los argumentos de los proveedores de equipos.

La incorporación de tecnología en el proceso fundante de nuestro sistema político no puede basarse en argumentos mágicos y expresiones de deseo: en estas condiciones, informatizar el proceso de emisión y recuento de votos equivale a privatizar la democracia. Ese es el riesgo de reducir a consignas simples, de pretendido "sentido común", un tema extremadamente complejo.

En la provincia de Buenos Aires esas consignas han abandonado incluso el terreno de la dialéctica mediática y se han incorporado a los textos de uso obligatorio para los alumnos de la Escuela Secundaria Básica. Dice un manual escolar editado por las autoridades educativas: "Voto electrónico: (en la provincia de Buenos Aires aún se hacen pruebas piloto) se trata de un sistema que permite realizar la votación a través de la Red Virtual. Tienen la enorme ventaja de tener bajo costo, rapidez en la obtención de los resultados, seguridad, transparencia en el proceso electoral y la eliminación de la posibilidad de fraude".[9]

Agrega esta sorprendente definición a la "Red Virtual"; suponiendo que se refiera a Internet, su utilización en los comicios está lejos siquiera de ser considerada hasta por los más entusiastas defensores del voto electrónico. También introduce una absurda consideración sobre hipotéticos ahorros que no vamos a detenernos en analizar toda vez que una urna de cartón puede comprarse por menos de $10 en comercios minoristas, monto impensado para un dispositivo electrónico sofisticado, y ello sin tener en cuenta los costos adicionales (adecuación de la infraestructura y otros).

Por supuesto, la tecnología puede ayudar a mejorar el proceso electoral en su conjunto. El desarrollo de mejores padrones y con mayor nivel de actualización es una necesidad más apremiante que la incorporación de urnas electrónicas. Un padrón más exacto facilitaría el rediseño de circuitos electorales más pequeños, acercando el lugar de votación al ciudadano. En la provincia de Buenos Aires la mayor parte de los circuitos electorales se mantiene igual desde hace más de cincuenta años. Muchas áreas rurales que por su escasa población daban lugar a circuitos electorales muy extensos se han transformado en áreas urbanas desde hace décadas sin que se haya modificado la geografía electoral; hoy tienen padrones de decenas de

miles de electores que deben movilizarse a sitios de votación alejados de su hogar.

Y sin que tenga ninguna relación con la tecnología de emisión del voto a utilizarse, hay algunos cambios que deben ser considerados seriamente. La vuelta a mesas electorales de 290 electores parece ser una necesidad apremiante. Si se ha aumentado la cantidad de electores por mesa debido a la falta endémica de autoridades dispuestas a cumplir con su deber, reducir la cantidad de mesas no parece ser la solución adecuada, toda vez que hace más ingrata la tarea y quienes pasen por esa experiencia se sumarán a las filas de los reticentes en la siguiente elección. Por otra parte, la escasez de autoridades de mesa condicionará los comicios cualquiera sea el sistema de votación que se utilice.

Lo mismo sucede con la logística de las elecciones: si los materiales de votación y los custodios del comicio llegan al lugar de votación varias horas tarde de poco servirá responsabilizar al sistema de votación por los problemas que esto ocasione.

Muchas de estas cuestiones se transforman en serias dificultades al momento de votar pero ninguna de ellas se soluciona con la incorporación del voto electrónico. Al contrario, el voto electrónico agrega nuevas dificultades y un problema insalvable: no es posible saber qué sucede dentro de la urna cuando apretamos “enter”.

Notas

1- http://www.lanacion.com.ar/nota.asp?nota_id=957482
2- http://www.lanacion.com.ar/nota.asp?nota_id=957476
3- http://www.lanacion.com.ar/nota.asp?nota_id=540075
4- http://www.clarin.com/diario/2003/10/26/um/m-647903.htm
5- http://www.elmundo.es/navegante/2006/11/08/tecnologia/1162977722.html
6- Que incluirían, aunque sin agotarse en ellas, sistema operativo de código abierto, software de votación de código abierto y hardware abierto, condiciones que los proveedores conocidos a la fecha no satisfacen.
7- Sólo como referencia, aunque no es el único estudio realizado: “Security Analysis of the Diebold AccuVote-TS Voting Machine” en http://itpolicy.princeton.edu/voting/ts-paper.pdf
8- http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/07/28/VOTING.TMP&tsp=1
9- Tecnología de la Información y la Comunicación, Cuaderno de Trabajo Nro 8. Dirección General de Cultura y Educación, Gobierno de la Provincia de Buenos Aires, Marzo de 2006. ISSN 1669-9211

* Patricio Lorente trabaja en la Universidad Nacional de La Plata, es activista de Software Libre, colaborador amigo de Fundación Vía Libre y actualmente preside la Asociación Wikimedia Argentina, capítulo local de la Fundación Wikimedia Internacional, organización que alberga proyectos Wiki tales como la Enciclopedia Libre Wikipedia, Wikimedia Commons, entre otros. Lorente es además bibliotecario de Wikipedia.

¿Qué necesitamos para confiar en un mecanismo de voto electrónico?

Federico Heinz

La pregunta

El entusiasmo por la adopción del voto electrónico es muy comprensible, si tenemos en cuenta que se da en un contexto en el que nuestras sociedades están incorporando dispositivos de procesamiento de datos a un ritmo sin precedentes y para un rango muy amplio de tareas. Algunos partidarios de las urnas electrónicas preguntan "si confiamos en cajeros automáticos y computadoras lo suficiente como para encomendarles transacciones que implican grandes cantidades de dinero, ¿por qué no confiar en ellas para nuestros votos?"

Responder a esta pregunta involucra reconocer la diferencia fundamental entre un cajero electrónico y una urna electrónica: el primero registra operaciones sometidas a un proceso muy estricto de auditoría, para el que es importante identificar lo mejor posible quién realizó cada una, mientras que en la urna lo importante es, precisamente, evitar la identificación del votante para preservar el secreto del voto.

Desde el punto de vista puramente técnico, la dificultad para realizar una urna electrónica confiable

reside, justamente, en el conflicto entre dos requisitos indispensables: que sea posible verificar que la urna operó correctamente durante el comicio, y al mismo tiempo sea imposible identificar a quién pertenece cada voto. Aún sin el requisito de auditabilidad, mantener el secreto del voto es muy difícil para la computadora: a diferencia del ser humano, la computadora tiene grandes dificultades para "olvidar."

Si el programa que controla la urna no "recuerda olvidar" todos y cada uno de los datos que permitirían reconstruir el vínculo de los votantes con el voto, tales como la secuencia o la hora en la que fueron emitidos, el secreto del voto puede ser violado con facilidad. Incluso cuando la máquina fue programada para olvidar esta información, es muy sencillo cometer errores que tienen como consecuencia que el olvido no sea permanente: borrar datos de manera que no puedan ser recuperados es una tarea bastante compleja, y reordenar el registro de votos de tal modo que sea imposible reconstruir su secuencia de emisión requiere de técnicas avanzadas de programación y dispositivos electrónicos cuyo correcto funcionamiento es imposible de verificar.

Aún así, la pregunta inicial no es ociosa. El hecho de que hayamos logrado mejorar la eficacia de muchas tareas usando computadoras sugiere que debería ser posible hacerlo también con la emisión del voto, y hay empresas e individuos empeñados en resolver el problema. Lo que debemos preguntarnos es, entonces, ¿cómo saber si una solución es aceptable o no? No tiene sentido aceptar las afirmaciones de quienes ofrecen los equipos ni escuchar opiniones que no estén fundamentadas en hechos concretos.

Necesitamos fijar un criterio medible, alguna característica concreta de la urna que, de ser satisfecha, nos garantice que podemos confiar en que el resultado calculado por la urna en el día del comicio es correcto. Lo palabra "medible" en la frase anterior es clave: quiere decir que la decisión de si la urna satisface o no la característica no puede ser materia opinable, sino que debe ser posible determinarlo sin lugar a dudas mediante un mecanismo científico.

¿Existe tal criterio?

Medir la confianza

La dificultad en encontrar un criterio que nos permita afirmar que el resultado de una urna electrónica es confiable reside en la misma naturaleza programable de estos dispositivos. Así como es posible incluir en el

programa sofisticados mecanismos para evitar la adulteración de los resultados, también es posible hacer lo propio con sistemas igualmente complejos, destinados a falsificar el resultado de manera que no sea detectable en una auditoría.

El criterio que inmediatamente acude a la mente es el de “probar a ver si anda” y, de hecho, uno de los argumentos más frecuentemente blandidos a favor de tal o cual urna electrónica es “lo probamos en tal lado y funcionó sin problemas.” En América Latina, este argumento se presenta por lo general como “lo usan en Brasil, y allí funcionó.”

Este abordaje presenta varios problemas:

- Estamos ante un ejemplo de razonamiento circular: “pensamos que funciona porque pensamos que funciona.” Es cierto, se usó en Brasil, pero ¿cómo sabemos que funcionó? ¿Qué mecanismo confiable e independiente de verificación fue utilizado para constatar que los resultados fueron, efectivamente, los que las urnas arrojaron? Es perfectamente posible que los votos emitidos en las elecciones “electrónicas” en Brasil hayan sido significativamente diferentes de los resultados obtenidos, pero al no haber una manera de contrastarlo con un registro independiente, no nos queda más remedio que suponer que funcionó.
- Aún si suponemos que determinado tipo de urna funcionó correctamente todas las veces que lo usaron, eso no quiere decir que lo hará la próxima vez que lo usen, o cuando lo usen en otro lado. El estado del arte en informática es tal que aún no sabemos cómo construir programas sin errores, y el hecho de que un error no se haya manifestado aún no quiere decir que no exista. No tenemos ninguna garantía de que una urna que funcionó bien en una elección con tres partidos seguirá haciéndolo con cinco, ni que lo hará cuando la cantidad de votantes sea significativamente mayor o menor, o cuando el horario del comicio sea de diez a dieciocho horas y no de ocho a dieciséis. Tampoco podemos estar seguros de que de una elección a otra no se haya descubierto (y mantenido en secreto) una vulnerabilidad hasta entonces desconocida.
- El que nadie haya explotado vulnerabilidades de una urna no quiere decir que no existan, ni siquiera quiere decir que sean desconocidas. De hecho, un atacante que deseara aprovechar una vulnerabilidad conocida por él en cierto modelo de urna haría todo lo posible por promocionarla y mostrar que funciona correctamente en cuantas pruebas se hagan, cuidándose mucho de no explotarla en elecciones poco importantes. De esa manera construye una confianza ficticia en el

dispositivo, para poder aprovechar la vulnerabilidad cuando se lo use en una elección importante.

- Las pruebas controladas no son comparables al caso de una elección real: es mucho más sencillo realizar una votación con pocas mesas, en un entorno vigilado por especialistas y donde el incentivo para atacar el sistema es bajo (por ejemplo en un concurso de belleza, o en una elección de intendente de un pueblo pequeño), que en una elección a gran escala en la que debemos suponer que los mismos fiscales que controlan el comicio pueden ser corruptos y en la que están en juego intereses poderosos. Además, es posible programar a la urna para que se comporte de una manera distinta durante las pruebas que durante una elección real.
- Las urnas electrónicas son sistemas complejos, y aún suponiendo que el programa que las controla calcula debidamente los resultados, es imposible asegurar que ninguno de sus componentes no relacionados directamente con el recuento de votos (el sistema operativo, los subsistemas de entrada/salida, etc.) está afectado por vulnerabilidades que permitan modificar el comportamiento del programa utilizando como vector un virus o gusano que se difunda entre las urnas durante el proceso de parametrización. Esta técnica permite a un atacante convertir a una urna confiable en una que no lo es, sin que nadie lo advierta.

Hay más objeciones a este argumento, pero podemos resumirlas en un principio: lo importante no es si la urna funcionó bien alguna vez o no, sino si funcionó bien durante este comicio. Una manera factible de realizar este control es hacer, el mismo día y a la misma hora que la elección real, una prueba paralela usando un subconjunto de urnas elegidas al azar en ese mismo momento, y en el lugar donde estaba planeado usarlas. Esta prueba paralela consistiría en realizar sobre esa urnas un simulacro de votación, contabilizando por fuera del sistema cada “voto” emitido para luego del acto electoral cotejarlos con los resultados de la urna.

Si bien esta prueba es significativamente más contundente que las mencionadas anteriormente, la logística para realizarla en forma correcta es tan complicada como para volverla impracticable: las urnas a auditar deben comenzar a operar al mismo tiempo que las demás, pero su selección al azar debe ser hecha en ese mismo momento, y no antes, lo que hace muy difícil ubicar a los auditores de tal modo que puedan realizar la prueba. También, es importante que el patrón de votos emitidos en la urna auditada se corresponda estadísticamente, tanto en distribución como en secuencia, con los votos que están siendo emitidos en las demás urnas, lo que es imposible de asegurar porque, si conociéramos los valores a los que

debemos aproximarnos, no necesitaríamos hacer la elección. Por lo demás, el mecanismo sigue siendo vulnerable a una programación que identifique si el patrón de votos es "sospechoso" de ser una auditoría y no una votación real, y que se comporte de manera diferente en cada caso.

Por supuesto, no somos los primeros en preguntarnos cuál sería un criterio aceptable para decidir si una urna es confiable o no. Un grupo de trabajo de especialistas convocados por el National Institute of Standards (NIST) de los Estados Unidos concluyó en el 2006, por ejemplo, que no sabían de ningún criterio medible que permitiera decidir si una urna es confiable o no. Sin embargo, siguieron estudiándolo, y en el 2007 lograron acordar un criterio que parece ser adecuado: puede decirse que una urna es confiable si puede obtenerse el resultado correcto independientemente del software que corre en la máquina.

Independencia del software

Para las personas que entienden el funcionamiento de las computadoras, el concepto de una urna electrónica que calcule un resultado correcto independientemente del software que ejecuta resulta absurda: la computadora siempre calculará siguiendo las instrucciones del software, y si éste la instruye de tal modo que dos más dos sea cinco, este será el resultado que la urna presentará, sin siquiera sonrojarse.

A lo que NIST se refiere con "independencia del software" no es a la construcción de urnas que se comportarán correctamente sin importar si el programa contiene errores o código malicioso (lo que sería imposible), sino de urnas que ofrezcan un mecanismo que permita calcular el resultado sin necesidad de recurrir al software. En otras palabras, una urna que lleve una contabilidad doble de los votos: una interna, digital, que es el la que el software usa para calcular sus resultados, y otra externa, analógica y legible por seres humanos sin asistencia técnica, que permite hacer un recuento independiente a mano.

Esta posibilidad es la que nos permite verificar, aún luego de realizado el comicio, si la urna se comportó correctamente o no: basta con tomar un muestreo aleatorio estadísticamente significativo de todas las urnas, y hacer un recuento manual. Si el resultado de todas las urnas auditadas es correcto, entonces podemos asegurar con alto grado de confianza que el resultado en todas las demás también debe haberlo sido. De lo contrario, debemos descartar el resultado calculado automáticamente, y

recontar todos los votos a mano. Afortunadamente, y a diferencia del caso de la urna electrónica sin registro paralelo, este recuento puede ser engorroso, pero al menos es factible.

Un ejemplo de tal sistema son los dispositivos de automatización del escrutinio, aquellos en los que el votante hace marcas sobre una boleta de papel que deposita en una urna, que los fiscales luego abren y recuentan pasando las boletas por la máquina. En este caso, las boletas de papel ofrecen un mecanismo alternativo de recuento. Otro ejemplo son las urnas electrónicas provistas de impresoras de boletas, en las que la boleta impresa también ofrece un respaldo razonable para el recuento, pero aquí hay que hacer la salvedad de que, dado que en éstas es la urna misma la que produce las boletas, existen posibilidades de ataque de demostrada eficacia en las que la urna facilita la vinculación de cada votante con su voto, o en las que la misma urna invalida boletas correspondientes a votos genuinos y emite votos falsos para reemplazarlos.

Existen también otros mecanismos posibles de urnas con registros independiente basados en mecanismos criptográficos de los llamados “end-to-end” (“de cabo a rabo” es una traducción razonable). No existen hoy más que algunos esbozos de cómo este tipo de urnas aseguradas con criptografía end-to-end podrían funcionar, de modo que la discusión alrededor de ellas seguramente será más académica que práctica durante algunos años.

Es poco lo que podemos decir hoy acerca de cómo serán estas máquinas cuando lleguen, pero hay una característica que seguramente las distinguirá, porque está en la base de toda la investigación en criptografía: sus mecanismos funcionarán sobre una base matemática muy compleja. Quienes la comprendan podrán, es cierto, decirnos si el mecanismo es sólido o no, y por qué. Pero quienes no la comprendamos no tendremos más remedio que confiar en ellos.

Quizás sea razonable confiar en la élite matemática del país, quizás no. Es uno de los muchos debates que nos debemos en torno al tema de las elecciones. Mientras tanto, queda claro que el consenso respecto de las urnas electrónicas es que no podemos saber si son confiables a menos que se limiten a contar votos emitidos en papel.

Auditoría, Secreto y Desmaterialización del Voto. ¿Es posible?

Pedro A. Dourado de Rezende*
Colaboración: Amílcar Brunazo Filho

Síntesis: Este artículo se propone compartir con el lector las principales lecciones aprendidas en la experiencia pionera de Brasil con la primera implementación total y universal de sistemas de voto electrónico del mundo. Los diferentes conceptos de "seguridad" juegan aquí un rol clave y ponen en claro contraste en la saga brasileña.

INTRODUCCIÓN

La cuestión central planteada por este artículo gira en torno de hasta qué punto podemos definir lo que es posible en materia de auditoría en estos nuevos procesos electorales electrónicos. De una forma más precisa, se trata de la pertinencia o de la necesidad -o no- de retener una representación física/tangible (impresión en papel) de cada voto emitido en el sistema, de modo de permitir la fiscalización manual del escrutinio.

El control de las elecciones gubernamentales procesadas electrónicamente ha sido discutido en todo el mundo en el ámbito académico, en Brasil, desde que se adoptaron las Urnas Electrónicas en 1996[1], con antecedentes a partir del caso ProConsult en 1982[2] durante las elecciones a gobernador en Río de Janeiro[3].

En los EEUU, donde la implementación del Proceso Electoral está definida por leyes de cada estado, este debate tuvo origen a fines de los años 80, ganando fuerza y espacio en los titulares de los principales medios de comunicación después del "fiasco de Florida" en el año 2000[4].

En Brasil hubo una situación similar durante dos breves períodos: para la inauguración del uso de computadoras durante el proceso de escrutinio en Rio de Janeiro en 1982 (mencionado anteriormente) y cuando fue alterado el "Panel Electrónico" del Senado[5] en 2001.

En los EEUU y en Europa, actualmente participan de esta discusión muchos especialistas que trabajan en informática y en seguridad de la información, además de algunos especialistas en ergonomía y en mecanismos de acceso. En su mayoría, son partidarios de la obligación de que las máquinas electrónicas impriman cada voto como un comprobante y referencia material y visual, y lo almacenen sin darle al elector posibilidad de interferir en el proceso.

El objetivo de esta medida de fiscalización consiste no sólo en posibilitar nuevos escrutinios de votos electrónicos (si así fuera requerido) sino también la posibilidad de guardar una prueba fidedigna de la transparencia del proceso electoral, como comprobante de confianza en el resultado logrado por la participación del elector, esencia del espíritu democrático, sea éste el de la antigua democracia griega o el de la democracia actual.

Participan también del debate sobre el proceso electoral electrónico oficiales de justicia y empleados de Tribunales Electorales, organizadores y ejecutores del Proceso Electoral que a veces -en su mayoría- son contrarios a esta medida de fiscalización, debido al trabajo extra que implica. Aunque raramente se admita en público, su oposición también se debe a la posibilidad de discrepancias entre el Escrutinio Electrónico y los controles manuales, que pueden manifestar incapacidad (ineptitud) o mala intención de estos funcionarios en el desempeño de sus funciones.

El nuevo rompecabezas de la Seguridad Electoral

Muchos especialistas en tecnología de la información defienden la idea de mantener el voto físico en los sistemas electorales electrónicos, porque los recursos científicos y técnicos disponibles o posibles para la seguridad computacional son insuficientes para ofrecer confiabilidad

en el resultado de la elección con voto secreto si los votos son procesados y recontados solamente de forma electrónica. Podemos citar algunos especialistas de TI, íconos vivos de la ciencia de la computación como Ronald Rivest (inventor del método RSA de firma digital), David Chaum (inventor del "dinero digital") y Bruce Schneier (criptógrafo y autor de grandes best-sellers sobre seguridad computacional).

Todos estos eminentes científicos han publicado artículos seminales, en los cuales explican por qué es más fácil, por ejemplo, proteger transacciones financieras contra fraudes electrónicos que el "escrutinio secreto" puramente electrónico dentro de los criterios máximos de seguridad. Esto nos lleva a reconocer que "seguridad" está siendo interpretada en dos sentidos diferentes: uno legítimo y el otro ilegítimo en relación al espíritu democrático:

El primer sentido es el de la seguridad de electores:

1. con derecho a voto y a un proceso limpio;
2. contra eventuales manipulaciones indebidas del proceso;
3. de cualquier origen o forma de vulnerar del sistema;
4. a través de la cual cualquier manipulación pueda ser detectada gracias a una fiscalización efectiva.

El segundo sentido corresponde al de la seguridad de los organizadores o ejecutores del proceso:

1. con derecho de acceso del sistema para programarlo, controlarlo y/o operarlo;
2. contra la eventual detección por medio de fiscalización;
3. de cualquier desliz por incapacidad (ineptitud) y/o mala intención;
4. a través de la cual se pueda sospechar que el proceso no fue limpio.

La arriesgada carrera por la modernidad

La dificultad relacionada a la seguridad encontrada por los autores -que defienden la seguridad electoral en el primer sentido- se encuentra relacionada a dos requisitos exigidos para desarrollar estos sistemas: el secreto y la

desmaterialización del voto, los que operan en un contexto que encierra por lo menos tres intereses potencialmente conflictivos: el de por lo menos dos candidaturas; y el de los electores que creen en la democracia a través de elecciones honestas o por lo menos así lo desean (en éste último grupo se encuentran los autores). Tal incongruencia torna inseparables estos dos sentidos de seguridad, ya que el primero, legítimo, sólo será eficaz conjugado con la negación del segundo: ilegítimo. O sea, la garantía de seguridad del proceso se dará sólo si el elector puede estar protegido también contra la posibilidad de fraudes de origen interno, por lo que, en caso que algún ejecutor del proceso decidiera actuar a favor de una práctica fraudulenta a su alcance, debería estar desprotegido.

Podemos preguntarnos, entonces, ¿dónde está el peligro? En los procesos en los que están en juego más de dos intereses, como el Electoral, los conflictos de interés presentan oportunidades de colusión. La colusión es un acción en la que dos o más intereses, opuestos o no, conspiran para engañar a otros en beneficio propio. En este caso, el engaño sirve incluso para despistar acerca de los reales intereses para elegir condiciones bajo las cuales los dos sentidos de seguridad anteriormente citados, legítimo e ilegítimo, se cancelan mutuamente al volverse parecidos. De allí a campo orégano de la colusión, hay un paso: camuflar seguridad del segundo tipo, para que se haga pasar por seguridad del primero. Por esto, la seguridad de los legítimos intereses en juego no puede, bajo riesgo de colusión, ser buscada en controles unilaterales del proceso o en el secreto de sus mecanismos. La protección contra el riesgo de colusión, al contrario, sólo es posible con un adecuado equilibrio entre la transparencia del proceso y la distribución de controles entre intereses legítimos y potencialmente conflictivos, a través de medidas reguladoras que puedan armonizarse e integrarse para constituir un (sub) proceso de fiscalización eficaz.

Por su naturaleza, este tipo de riesgo amenaza cualquier democracia. Según nos enseñan los libros de historia, contaminaban a la Vieja República en el Brasil[7]. En ella, la colusión involucraba la organización del proceso y de dos candidaturas que ocultaban el previo acuerdo secreto sobre el resultado a ser divulgado y que alternaban a los dos partidos en el gobierno, independientemente de la votación. Se lo llamaba "política café con leche". El pueblo brasileño soportó décadas acumulando las consecuencias nefastas de esto, demora que nos llevó a la revolución del 30, buscando un perfeccionamiento democrático. Dos interrupciones del régimen democrático más tarde, actualmente bajo la fascinación de las tecnologías de la información -vendidas como panacea contra todas las miserias humanas- las lecciones de la Vieja República parecen olvidadas. Estas tecnologías maravillosas y sus sistemas desmaterializadores, capaces de capitalizar la inmaterialidad del voto en agilidad y rapidez para el

escrutinio nos están siendo vendidas, a un precio muy alto, como irrefrenable modernidad y como moderna protección contra las antiguas formas de fraude. Como si eso constituyese un bien en sí mismo. ¿Lo será?

DOS LADOS DE UNA MISMA MONEDA ... QUE NO GIRA

En elecciones secretas, en las cuales la identidad del votante no puede ser vinculada a su voto durante la votación ni durante el escrutinio, la eficacia del proceso de fiscalización se torna sensible al soporte que registra materialmente cada voto. En consecuencia, si el proceso de votación electrónica desmaterializa el voto, registrándolo — a cada voto o a sus sumas parciales — sólo digitalmente, la eficacia de cualquier proceso de fiscalización se ve anulada. Anulada en el sentido de que cualquier medida para detectar o impedir fraudes de origen interno (colusiones entre un organizador y alguna candidatura) servirá también para proteger a los defraudadores externos, fiscales de candidaturas empeñados en sabotear (anular una elección perdida) o subvertir la fiscalización (contaminar el sistema con mecanismos de fraude). Al mismo tiempo, cualquier medida para detectar o impedir sabotaje o subversión del resultado final en la fiscalización protegerá también a los defraudadores de origen interno que tengan privilegios de acceso para programar, controlar u operar el sistema. Se trata de la incongruente lucha entre espías y contra-espías, que une los sentidos legítimos e ilegítimos de la seguridad.

Quien como ciudadano no se preocupa por el riesgo de que la seguridad legítima sea, bajo algún pretexto, arrollada por la ilegítima, no valora la democracia o, en el fondo, no la acepta. Y quien, como científico, desee estudiar sus mecanismos, debe separar tal conocimiento y creencias de los problemas y límites inherentes a los mismos. Así fue que el estudio científico de esos límites alcanzó un marco importante con la tesis de doctorado de la Dra. Rebecca Mercury, defendida en la Universidad de Pensilvania (EUA) en el año 2000[8]. Su tesis muestra que la inviolabilidad del secreto del voto y la garantía del correcto escrutinio -garantía que niega el segundo sentido de más arriba- son propiedades excluyentes en los sistemas puramente electrónicos. En otras palabras: en una elección procesada sólo electrónicamente, es imposible asegurar a la vez el secreto del voto y la corrección del escrutinio, pues en ella tales protecciones son como fases opuestas de una misma moneda. Moneda que corresponde al sistema electrónico puro, cuyo valor corresponde al proceso electoral que el sistema ejecuta, pero moneda que no se puede “girar” durante una elección para poder ver sus dos lados, pues el proceso es ejecutado sin posibilidad de auditoría.

El peso de estos argumentos científicos pasó a reflejarse, bajo presión de movimientos civiles[9] fortalecidos por la dudosa ética de los proveedores de sistemas electrónicos puros, en la legislación electoral norteamericana. Entre marzo de 2004 y mayo de 2005, 14 estados federales aprobaron leyes que obligaban a las máquinas electrónicas de votación a emitir un voto impreso y verificable por el elector, para mantener o recuperar capacidad de auditoría del proceso electoral anterior a las computadoras. Hoy 19 estados ya tienen leyes de este tipo aprobadas, 3 están esperando ser sancionadas, 17 tienen proyectos en trámite y solamente 12 no ven problemas en usar máquinas del tipo que Brasil usa hoy. Por otro lado, en el Congreso están siendo tramitadas hoy casi una decena de proyectos exigiendo el voto impreso verificable por el elector como parte del principio federal de organización democrática en los EEUU. La idea no es, ingenuamente, la de acabar con los fraudes, pero sí la de hacer que sus posibles formas sean más difíciles, costosas y arriesgadas en igual medida, exponiéndolas al riesgo de ser comprobadas a tiempo y por electores comunes, incluso aquellos que no tienen doctorados en seguridad informática.

EL CAMINO DEL VOTO ELECTRÓNICO EN BRASIL

En Brasil, la implantación del voto electrónico ha seguido otros caminos. La transparencia del proceso electoral y de su organización, la del proceso de formación de sus leyes y reglamentos y la participación en éstos de la sociedad civil han dejado mucho que desear, incluso frente a las mismas dudas éticas sobre los mismos proveedores de sistemas electrónicos puros. Esto se debe, en buena parte, a la peculiar organización jurídica de Brasil, tal vez la única de las democracias republicanas del mundo que acumula las funciones de reglamentacion, ejecución y fiscalización -roles que una república debería mantener separados- del proceso electoral en una sóla institución: la "Justicia Electoral" al mando del Tribunal Supremo Electoral (TSE).

La Ley 9.100 de 1995 -que permitió el uso del voto electrónico- y la Ley 10.740 de 2000, que puso fin al voto impreso verificable por el Elector, fueron elaboradas dentro del TSE. Ambas normas fueron aprobadas, siempre bajo presión de algunos de sus ministros, en el Congreso Nacional con participación significativa de parlamentarios envueltos en litigios con la propia la Justicia Electoral, y sancionadas en menos de 6 meses de trámite, sin que se permitiera una sola audiencia pública. En la elaboración, aprobación y sanción de estas leyes, todas las

contribuciones al debate ofrecidas por la comunidad académica fueron despreciadas, incluyendo:

1. Manifiesto de los Profesores Universitarios, hoy con más de 1.700 firmas[12], advirtiendo a los parlamentarios y a la sociedad sobre los riesgos del sistema electoral electrónico que no permite auditoria del escrutinio, y solicitando que durante los debates para legalizarlo hubiese audiencias públicas.
2. Informes de la Sociedad Brasileña de Computación (SBC) y de la Fundación COPPETEC de la Universidad de Río de Janeiro/UFRJ, con evaluaciones bastante críticas del sistema en uso y uno de ellos (el de la SBC[13]) recomendando la impresión de cada voto para que pudiese ser verificado visualmente por el elector, sin que éste pudiera interferir con él, de modo de tornar auditable el proceso del escrutinio final de los votos;
3. Pericia técnica de Santo Estevão, Bahia, (parte del proceso TER-BA 405/2000, que solicitaba la anulación del Escrutinio municipal de esta ciudad).[14]

REDUCCIONISMO

Estos documentos señalan graves fallas de seguridad (en el primer sentido) que posteriormente pudieron ser comprobadas, cuando una parte del software usado en urnas en la elección brasileña de 2000 se filtrara en Internet, fuera analizado por uno de los autores del presente artículo, y terminara siendo identificado como el software analizado en la pericia de Santo Estevão. El análisis e identificación de la parte analizada, precisamente la que controla la seguridad lógica de la urna (su setup), mostró cuán ridículo era el proceso de fiscalización[15], y aún así no despertó interés en la opinión pública. La comprobación sólo fue posible gracias a una ruptura momentánea del oscurantismo que rodea al sistema electoral brasileño, por mucho que algunos confundan ese oscurantismo con seguridad, y a esa ruptura con violación. Ese oscurantismo sirve en realidad para camuflar el segundo sentido de la seguridad para que aparente ser el primero.

El último documento (la pericia técnica), registrado en un proceso de impugnación electoral de Santo Estevão, es de extrema importancia pues relata la única pericia hasta hoy ejecutada por un técnico independiente sobre una urna electrónica usada en elecciones oficiales en el Brasil. La

pericia realizada en Santo Estevão muestra, entre otros hechos, la absoluta ineficacia — en el primer sentido de seguridad mencionado arriba — del sistema de precintos físicos entonces utilizado en la urna electrónica brasileña, conjugada con su absoluta eficacia en el segundo sentido. También revela cómo el lenguaje de la reglamentación oficial de esos sistemas de precintos y de los alardes oficiales sobre la seguridad que proporcionan puede servir para camuflar el segundo sentido de seguridad con la apariencia del primero. El referido documento de Santo Estevão es esencial en el rompecabezas de revelar como esa apariencia es sostenida: a base de toscos alardes, ignorancia colectiva y de prepotencia reduccionista (ignorancia de la propia ignorancia).

Algunos son víctimas de ese reduccionismo al confundir el sistema electrónico con el proceso electoral, o al confundir el secreto del voto con el secreto en el proceso que recoge y suma los votos (por cargos, secciones, unidades) y divulga los resultados. Otros, al confiar en un pálpito de que la transparencia actual ya es suficiente, quizás porque no saben para qué serviría más transparencia, o qué hacer con ella. Otros aún, creyendo una intuición de que más transparencia perjudicaría la seguridad, definida en forma vaga e imprecisa, cuando no maniqueísta (¡los hackers de Internet!). Para agravar la situación, están los especialistas[16] de cátedra y de oportunidad, con ambiciones turbias y pocos escrúpulos, empeñados en explotar ese reduccionismo como si la urna electoral fuese una cajita de mago. Es aquí donde surge la necesidad de acabar con ese oscurantismo, para que podamos ver cómo, en sistemas puramente electrónicos de votación secreta, esos dos sentidos de seguridad -legítimo e ilegítimo- no sólo se vuelven inseparables y mutuamente cancelantes, sino que, peor todavía, se pueden volver peligrosamente parecidos.

La salvación según la Secta de San Byte [17]

Estos sistemas habrían encantado a Maquiavelo si hubiesen existido en el Renacimiento, principalmente por la pujanza de la Secta de San Byte[18], el nuevo credo que surge con ellos. Surge al transformar en dogma las corazonadas que circulan en la medios de comunicación sobre lo que es transparencia suficiente en los sistemas electrónicos, para revelar una realidad diferente, teñida de rosa. La Secta de San Byte revela cómo el reduccionismo, consagrado por el poder pleno y absoluto de la Justicia Electoral, puede "salvar" nuestra democracia de las miserias humanas, a través de la fe en la inseparabilidad de

aquellos dos sentidos, alcanzada a través de la omnipresente pureza electrónica que nos permite eliminar para siempre el mal que nos atormenta desde milenios (¡hasta para difundir la Biblia!), el diabólico papel. Fe ééésta que protege de la tentación s redime del pecado de colusión a aquel que, en el ejercicio del poder electoral, programa, controla u opera su sistema electrónico puro (libre de la maldición del papel). O tal vez, en su ramificación fariseica, fe que explica, bajo sofisticados argumentos de autoridad[19], esos dos sentidos de seguridad como uno solo.

Basta ingerir, por los ojos y oídos, el brebaje ofrecido por los medios de comunicación corporativos, en el altar del consumo en nuestros propios hogares, para alcanzar la visión: seres angelicales programando, configurando, operando maquinitas …

Entre las señales de esta revelación mística, podemos citar:

1. La contaminación dogmática de estudios, pagados y dirigidos por el Tribunal Superior Electoral, sobre la seguridad del sistema (ejemplo: el carísimo estudio "de la UNICAMP[20]" de 2002, visto a la luz del análisis de su setup en el 2004[21]);
2. El veto a la participación de la Dra. Mercury en un evento científico sobre elecciones electrónicas, realizado en el 2003 en la Universidad Federal de Santa Catarina (UFSC) con el auspicio del TSE, bajo el pretexto de que ella no tendría nada para aportar al "perfeccionamiento de nuestro sistema";
3. La negación sistemática del TSE a permitir que representantes de los partidos políticos realicen pruebas independientes de penetración, como lo establecen las normas técnicas nacionales e internacionales para homologación de seguridad de sistemas electrónicos.

La tercera señal, la negativa a permitir pruebas homologatorias independientes legitimadas por estándares técnico-científicos, parece impresionante. Se la justifica, en un argumento autorreferente y evasivo, con la excusa de que el reglamento del Sistema Electoral Brasileño, elaborado por los propios fiscalizados, no las prevé. Las únicas pruebas legalmente permitidas son aquellas que la sapiencia insuperable e incorruptible de los mismos define, las cuales están limitadas a la participación de los fiscales en la mera observación de urnas, emitiendo informes de auto-indulgencia. El valor de nuestra moneda electoral estaría, de esta forma, basada únicamente en la palabra de

quien, investido de la capacidad legalista de aquel Poder electoral, ejerce simultáneamente sacerdocio en la Secta de San Byte. Algunas veces, en la palabra del mismo que declara, después de haber estado al frente de la Justicia Electoral, haber contrabandeado dispositivos no votados para la Constitución Federal, mientras era legislador constituyente. Y que responde, a aquellos que puedan sentir indignación: Lo siento mucho, mala suerte para los que firmaron abajo (firmaron en papel)[22]. Quien no se impresiona con esto, puede esperar las próximas señales.

Estos hechos, peripecias o herejías, no despiertan el "interés periodístico" en los grandes medios de comunicación, que ya están ocupados protegiendo a las masas contra el riesgo de la "falta de confianza" en el sistema, en arrebatarlas en burdos alardes recitando el mantra de San Byte: "¡nuestra urna pionera es segura!". O recitando el mantra de los fundamentalistas de la secta: "¡la Urna es 100% segura, porque si no lo fuera, habría pruebas de fraude!" O tal vez porque ya está ocupada con las peripecias de los publicitarios, proxenetas y políticos, y en identificar cuidadosamente cuáles de ellas interesan al público. Mientras tanto, el debate sobre la seguridad electoral, sobre las nuevas formas de fraude que, con potencia más concentrada y demoledora que las antiguas, nace de entregar eficacia fiscalizadora a cambio de agilidad en el conteo de los votos, es farisaicamente silenciado bajo la bendición del cuarto Poder[23]. A pesar de esto, las lecciones de la Vieja República, validadas en la Revolución del 30 en el mensaje de la bandera de la provincia de Paraiba, no han sido olvidadas por todos. Ni el hecho de que legalidad y legitimidad sean cosas diferentes.

Lecciones de Historia

Todavía algunos se ocupan en recordar la Historia, entre algunos motivos para evitar la repetición de los mismos errores históricos. Y esos, al volver los ojos hacia nuestro continente, ven una posición ambigua hasta en la Organización de los Estados Americanos (OEA). La OEA exigió a Venezuela, el único país del mundo que había adoptado las urnas electrónicas con voto impreso en la elección de 2004, que el resultado fuese auditado con escrutinio por recuento manual de los votos impresos de 1,5% de las Secciones Electorales. Se trataba del referéndum que podría derrocar a Chávez en Venezuela, en agosto de 2004. Para los demás países latino-americanos, la OEA sugiere y en algunos casos hasta intermedia, el uso del sistema electrónico brasileño, que no permite recuento manual ni auditoria del proceso.

Podemos intentar una respuesta al interrogante que

encabeza este artículo. Tomando como punto de partida no sólo los discursos oficiales y de los grandes medios de comunicación, con sus dobles varas a la hora de medir las maravillas tecnológicas en el proceso democrático, sino también el origen de los componentes, programas y contratos utilizados en el Brasil, la elección electrónica seria:

1. con auditoría del escrutinio, la mejor alternativa, para EEUU, país fundador de la democracia moderna, y para aquellos países de América Latina, fundada sobre un colonialismo sempiterno, cuyas democracias el gobierno de Washington estuviera explícitamente interesado en tutelar[24];
2. sin auditoria del escrutinio, la alternativa para países donde conviene que la tutela[25] no sea tan explícita.

Eso creen (quizás sin la tutela) las masas de maniobra del Brasil, las carnes de cañón de la modernidad electoral que aportan el gusto a sangre en la boca de los buitres, los cipayos y sus tutores fascistas. Quedan sólo los huesos duros de roer.

Notas

1- Las Urnas para Votación Electrónica en Brasil surgieron en el año 1996. Esta Urna electrónica está definida como "equipamiento electrónico para votación", el cual consta especialmente de un equipamiento compuesto por un colector electrónico de voto (2), conteniendo teclado y un display alfanumérico, el cual estará conectado a un micro-terminal (1) que permite al presidente de mesa realizar todas las operaciones de control del proceso de votación; el referido colector electrónico de voto teniendo acoplada en la salida de la impresora una Urna descartable, donde los votos son recogidos; con este equipamiento, la votación se torna electrónica, con el objetivo de disminuir el fraude electoral y agilizar el proceso global de votación y escrutinio; siendo que el citado equipamiento está dotado, también, de una lógica electrónica especialmente desarrollada para el mencionado aplicativo en cuestión. Su creador, el Ingeniero Carlos Rocha Moretzsohn firmó contrato con la empresa Unysis Brasil en marzo de 1996. El depósito del pedido de patente de la invención de la urna electrónica brasileña, fue depositado en el Instituto Nacional de Propiedad Intelectual/INPI, en junio de 1996, para poder atender a los compromisos definidos, en el mencionado contrato, bajo pedido:PI9601961-1 (22)

2- http://www.pdt.org.br/noticias/proconsult.asp

3- Leonel Brizola del Partido Demócrata Trabalhista/PDT (Partido Demócrata Laboral) y Wellington Moreira Franco del Partido Movimento Democratico Brasileño/PMDB - http://www.pdt.org.br/personalidades/bzelecfraud.htm

4- http://en.wikipedia.org/wiki/Butterfly_ballot

5- Puede ser consultado el documento de la OEA http://scm.oas.org/doc_public/PORTUGUESE/HIST_06/CP16506P08.doc. Documento do Conselho Permanente da OEA/Ser.G Organização dos Estados Americanos Cp/Cajp-

2320/05 Add. 2 do 23 maio 2006 da Comissão de Assuntos Jurídicos e Políticos Original: espanhol . (Relatório da reunião do 28 de abril de 2006 da Sessão especial da Comissão de Assuntos Jurídicos e Políticos destinada a promover, divulgar e intercambiar experiências e conhecimentos relativos ao acesso à informação pública e sua relação com a participação do cidadão, com a participação de peritos dos Estados e representantes da sociedade civil).

6- del verbo conchabar, pág.708 extraído del Diccionario de Uso del Español de Maria MOLINER A-G Madrid, Ed:Gredos (1980)

7- Período entre la proclamación de la República en 1889 y la revolución del 30. Durante la Vieja República estas alianzas de intereses comprometían la organización del proceso y sus Candidaturas, que ocultaban previos conchabos del resultado a ser divulgado, y que a cada elección alternaban en el Poder sus respectivos Partidos Políticos, independientemente de la Votación. Esto era conocido como la "política del café con leche" (asociando el café a San Pablo y la leche a Minas Gerais.

8- http://www.notablesoftware.com/Papers/thesdefabs.html

9 http://www.verifiedvoting.org/

12- http://www.votoseguro.com/alertaprofessores

13- Informe de la Sociedad Brasileña de Computación/SBC ... http://www.sbc.org.br/index.php?language=1&subject=1&content=downloads&id=51.

14- http://www.brunazo.eng.br/voto-e/textos/stoestevao1.htm

15- http://www.cic.unb.br/docentes/pedro/trabs/catsumi.html

16- http://www.cic.unb.br/docentes/pedro/trabs/relunicamp.htm

17- Analogía con el Santo Daime, nombre de una secta de seguidores y bebedores de Ayahuasca en Brasil.

18- http://www.cic.unb.br/docentes/pedro/trabs/azeredo.htm

19- http://www.cic.unb.br/docentes/pedro/trabs/paisagem.htm#9

20- UNICAMP: Universidad de Campinas en San Pablo.

21- http://www.cic.unb.br/docentes/pedro/trabs/analise_setup.html

22- Benayon, A. & Rezende, P.A. D.: "Anatormia de Uma fraude à Constituição", http://www.cic.unb.br/docentes/pedro/trabs/fraudeac.html

23- http://www.cic.unb.br/docentes/pedro/trabs/zileide.html

24- http://www.whitehouse.gov/nsc/nss.pdf

25- http://context.themoscowtimes.com/stories/2002/09/20/120.html

SOBRE LOS AUTORES

Pedro Antonio Dourado de Rezende, es matemático, profesor del curso de Ciencias de la Computación en la Universidad de Brasilia, Coordinador del Programa de Extensión en Criptografia y Seguridad en Computación de la Universidad de Brasilia, tambien es representante de la Sociedad civil en el Comité Gestor de Infraestructura de Llaves Públicas brasileñas (www.cic.unb.br/docentes/pedro/sd.htm)

Amilcar Brunazo Filho (Colaborador), es ingeniero, representante Técnico del Partido Socialista Brasileño y Partido Demócrata Trabalhista (Partido Demócrata Laboral) es Coordinador del Forum sobre Voto Electrónico, ver Internet (www.votoseguro.org).

Traducción: Blanca Nidia Lucero de Lazarte
Corrección de Traducción: Fundación Vía Libre

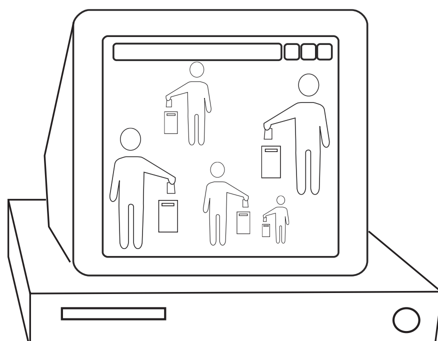
Artículo presentado en el V Coloquio Internacional sobre Votación Electrónica. Monterrey México Sep 2007

Derechos

Histórico de este Artículo

v1.0 5/7/05 Versión en Portugues publicado en el Observatorio da Imprensa (www.observatoriodaimprensa.org.br)
v1.1 9/7/05 Revisión del texto de la v1.0 publicada en el Portal Conciencia (www.comciencia.org.br) y en el Portal del IBDI (www.ibdi.org.br)
v.2 23/7/05 Revisión del texto de la v1.1., archivada en (www.cic.unb.br/docentes/pedro/trabs/u-e-auditoria.html)
v.3 15/6/07 Adaptación e Traducción al Español por Blanca Nidia Lucero de Lazarte
v.3.1 - 28/09/08 - Adaptación para publicación y corrección de traducción al español: Fundación Vía Libre Argentina

en los medios



Problemas con las máquinas de voto en EEUU

Retrasos en los cierres de muchos colegios

EFE | ELMUNDO.ES

WASHINGTON | MADRID.- Los problemas con el sistema de votación electrónica con el que han votado más del 80% de los participantes estadounidenses obligó a posponer el cierre de los colegios electorales en varias circunscripciones, algo que ya se venía anunciando.

En algunos estados, como Colorado o Indiana, las colas de gente que esperaba para votar sobrepasaban en algunos lugares las 300 personas, y muchos de ellos fueron enviados a sus casas para regresar más tarde.

En Denver, por ejemplo, el 'software' usado para la votación electrónica falló en varias ocasiones y los servidores sufrieron sobrecargas debido al número extra de líneas, según informa el distrito Denver Post.

Por esta razón, los jueces decretaron en varios estados que los centros electorales cerrasen más tarde, mientras que en otros la votación electrónica se sustituyó por las tradicionales papeletas. En la mayoría de los casos, los jueces emitieron su resolución a instancias del Partido Demócrata.

Uno de cada tres electores votaba en una máquina que jamás había utilizado antes, ya que durante la jornada expiraba el plazo para implantar la ley federal 'Ayuda a EEUU a Votar'.

Algún votante no acabó de digerir demasiado bien los problemas con las máquinas, como un hombre de 43 años que la emprendió a golpes con un pisapapeles contra uno de estos aparatos en Pensilvania y fue detenido por la policía. Cada una de las máquinas está valorada en torno a unos 5.000 dólares.

La tecnología jugó también una mala pasada en Carolina del Sur, donde se cayó la página web habilitada para las elecciones, que incluye información sobre los candidatos y las propuestas sometidas a referéndum, sobre los procesos de votación y sobre la ubicación de los colegios electorales.

Los blogs vigilan

Por supuesto, los blogs han tenido un protagonismo indudable en estas elecciones estadounidenses, como ya sucedió por primera vez en las presidenciales de 2004.

En esta ocasión, y durante la jornada electoral, varios weblogs informaron de posibles irregularidades o anomalías en los colegios electorales, a modo de 'guardianes de la democracia'.

Algunos ejemplos, que menciona 'New York Times', son RedState.com, que denunció problemas con las máquinas en Pensilvania, o Brad Friedman, muy crítico con este sistema de voto, quien se hizo eco de múltiples incidencias a lo largo del país.

Las bitácoras digitales albergan a todo el espectro político, desde las páginas más izquierdistas, como 'DailyKos', a auténticos paladines de la causa conservadora, como 'Instapundit'.

Mención aparte merece el ex empleado de supermercado reconvertido en líder de opinión, Matt Drudge, quien, por medio del sensacionalismo y un estilo punzante, ha conseguido que su 'Drudge Report' sea una de las páginas más visitadas en los despachos del poder en Washington.

Fuente:
Elmundo.es © Mundinteractivos, S.A.
http://www.elmundo.es/navegante/2006/11/08/tecnologia/1162977722.html

Diebold publica la 'llave' de las urnas electrónicas

Anne Broache

Imaginen si todo lo que hiciera falta para penetrar las máquinas de votación electrónicas Diebold, tal vez con intenciones maliciosas como instalar algún tipo de software que altere los resultados en su memoria, fuera una fotografía de la llave que otorga acceso físico a estos aparados usados masivamente.

Gracias a una pequeña ayuda de la empresa misma, esto puede ser realmente simple, tal como lo indicó un investigador en seguridad de la Universidad de Princeton esta semana.

De acuerdo con las declaraciones de J.Alex Halderman, un estudiante de PhD en Ciencias de la Computación, una foto de la llave publicada en la tienda en línea de Diebold era una llave real y verificable que permitía, si se la reproducía exactamente, abrir el acceso físico de las urnas electrónicas.

El que se ocupó de advertir este suceso fue Ross Kinard, del sitio SploitCast, que se autodenomina un 'podcast para hackers, geeks y paranoicos de la seguridad'. Kinard envió por correo tres copias caseras de las llaves a Halderman, quien comprobó con éxito que las mismas servían para desbloquear las máquinas Diebold AccuVote-TS.

Halderman tenía esas máquinas a mano porque junto a sus colegas de Princeton estuvieron probando la seguridad de este modelo de máquinas de votación sin papel que ha sido usado en por lo menos el 10% de la población electoral el año pasado.

Al mismo tiempo, indicaron que es cuestión de segundos llegar a uno de los dispositivos que guardan la memoria y abrirlo con estas llaves típicamente usadas en minibares de hoteles. Con menos de un minuto de tiempo de acceso físico al dispositivo, una persona con malas intenciones podría instalar software que corrompa las memorias internas, indicó el estudio presentado por Princeton.[...]

Fuente:

 http://news.cnet.com/8301-10784_3-6153328-7.html

Introduzca el sobre en la urna, pero guarda que patea

El lado oscuro del voto electrónico

Beatriz Busaniche*

Este artículo fue publicado en la página central de Diario Crítica de la Argentina, en su edición impresa del viernes 18 de abril de 2008.

Se lo presenta como la panacea de la modernidad, pero abre la posibilidad de fraude y de violación del secreto de sufragio. Hasta el rol del Estado puede desdibujarse cuando las empresas impiden auditar sus sistemas para "proteger la propiedad intelectual". La mayoría de las denuncias sobre irregularidades en el sistema de voto electrónico provienen de los Estados Unidos. Pero también las hubo en Holanda, Irlanda, Brasil. Los papelones ya llegaron a Tierra del Fuego y Río Negro.

En la Ciudad de Buenos Aires –en la que ya se hicieron experiencias piloto anteriores a la gestión macrista– el oficialismo, a través de Cristian Ritondo, promete que para 2009 los porteños votarán usando urnas electrónicas. En el Congreso, en marzo pasado, legisladores del Frejuli, el partido de Alberto Rodríguez Saa, presentaron un proyecto similar para la escala nacional. Algunos dirigentes de izquierda y miembros de la Coalición Cívica rescatan la idea como positiva. Por alguna razón se ha instalado la creencia de que el voto electrónico es la solución universal a los problemas electorales de la democracia.

Casi todo el espectro político, usando diversos argumentos, ve con simpatía lo que se muestra como una panacea. Pero nadie parece escuchar la voz de los especialistas en seguridad informática que advierten que el voto electrónico no es seguro. Un gran número de experiencias fallidas –muchas de ellas denunciadas en EE.UU. y con escándalo– muestra que las urnas electrónicas pueden poner en riesgo derechos básicos de la democracia, abrir la posibilidad de fraude y quebrar el secreto del sufragio.

El uso de sistemas informáticos en procesos electorales es común en los centros encargados de tabular los resultados generales. Pero el voto electrónico implica llevar la informatización al acto mismo de

emisión del sufragio. Según este modelo, los ciudadanos eligen el candidato en una pantalla y la máquina suma su voto de manera automática. El nuevo mecanismo, se argumenta, erradicaría los problemas del conteo manual y el robo de boletas.

Además, terminaría con el llamado "voto en cadena". Según algunos partidos minoritarios, tampoco haría falta tener fiscales de todos los partidos en todas las mesas porque los resultados se obtendrían inmediatamente, apretando un botón al finalizar el horario de votación. ¿Santo remedio para nuestra golpeada democracia?

Un regalo para George W. Bush

La cantidad de denuncias de fraude en los distritos de Ohio y Florida, tanto en las elecciones de 2000 como en las de 2004, es tanta que es imposible reproducirlas en dos páginas. Pero hay una constante: en todos los casos hay urnas electrónicas involucradas. De hecho, el ex CEO de Diebold, Walden O'Dell, se hizo famoso no sólo por ser uno de los grandes aportantes financieros a la campaña por la reelección de Bush, sino por haber dicho, en una invitación a una cena de recaudación de fondos para los republicanos, que se comprometía a "entregar los votos de Ohio al señor presidente".

Diebold era una de las firmas que se repartían el mercado de las urnas electrónicas en los EE.UU. "Era", porque Diebold como tal ya no está en el negocio. Tras numerosos escándalos, la firma decidió cambiar de marca para su división de servicios electorales. Ahora Diebold se llama Premier Elections Solutions Inc.

La cadena HBO realizó hace un par de años un documental titulado Hacking Democracy en el que se relata la historia de un grupo de ciudadanos preocupados por estos problemas. El documental, disponible en la red , revela en forma contundente las grietas de seguridad de las urnas usadas y muestra una larga serie de irregularidades. Al escándalo desatado por las preferencias políticas del CEO de Diebold se suman problemas en las urnas y dificultades para emitir el voto en distritos con alta concurrencia de votantes afroamericanos (distritos de mayoría demócrata) o las vulnerabilidades del sistema GEMS, la tabuladora central que se ocupa de sumar los votos emitidos.

En la Universidad de Princeton, el Center for Information Technology Policy dirigido por Edward Felten, profesor de Ciencias de la Computación y Asuntos Públicos, realizó una serie de pruebas de seguridad sobre las urnas Diebold AccuVote Systems. Los expertos pudieron manipularlas en minutos sin dejar huella del fraude. Inyectaron un virus en una de ellas, lograron que se reproduzca, modifique los resultados y se autoelimine para que no queden pruebas. Ningún trabajador electoral encargado de auditar el proceso tendría capacidad alguna para detectar esta manipulación. Lo que se demostró es que la tarea del fiscal perdía todo sentido.

Ante las denuncias, el Estado de California encargó una auditoría de seguridad sobre todas las urnas electrónicas usadas en ese distrito. Ninguna de las máquinas superó las pruebas realizadas por expertos de la Universidad de California. Los investigadores lograron superar sin mayores inconvenientes todos los sistemas de seguridad tanto en hardware como en software de todas las urnas evaluadas. La revisión incluyó equipos de votación de todas las compañías autorizadas para vender urnas en ese Estado, salvo ES&S, que no entregó los equipos a tiempo.

QUIÉN DIJO QUE EL VOTO ERA SECRETO

Una de las urnas que no aprobó las auditorías de la UCLA pertenece a la firma ES&S, protagonista de otro affaire en el Estado de Ohio, donde según un informe público, las urnas permiten violar el secreto del sufragio. Según explicaron los especialistas, la ley del Estado de Ohio permite a cualquier persona solicitar y obtener dos documentos: una lista de votantes y una lista de votos. El problema es que la urna entrega ambas listas en orden cronológico de emisión de voto. La combinación de estos dos documentos muestra quién votó por cuál candidato.

El problema no es que esos documentos estén disponibles al público, sino su mera existencia. El hecho de que las máquinas de votación tengan la capacidad de emitir este tipo de listados las invalida como garantes de privacidad en los sistemas de votación. Este mismo sistema se usa en alrededor de 20 Estados de los EE.UU.

En Holanda, violar el secreto del voto también es posible. Desde unos 25 metros de distancia es posible identificar por quién está votando una persona sólo decodificando las emisiones radioeléctricas de la urna.

Un principio de la democracia es el derecho a elegir y ser elegidos. Pero además, los ciudadanos tenemos derecho a auditar las elecciones y a comprender cómo funciona el procedimiento por el cual elegimos a nuestros representantes. En la actualidad, auditar una elección no requiere ningún conocimiento que la escuela pública no otorgue: leer, escribir y hacer operaciones matemáticas básicas. Maestros y funcionarios públicos son convocados a ejercer este derecho en nuestro nombre y los partidos políticos envían sus fiscales a las mesas de votación para el mismo fin. Cualquiera de nosotros puede participar de este proceso.

Una vez establecido un sistema de voto electrónico, la auditoría es mucho más compleja. Auditar un sistema de esta naturaleza será posible sólo para aquellos técnicos altamente capacitados que puedan leer el código fuente del programa –si el código está disponible–, detectar "puertas traseras" y evaluar el hardware. Muchos expertos en seguridad informática se declaran incompetentes para semejante tarea. En Brasil, los profesores de informática y computación han sido los primeros en dar la voz de alerta.

Un caso interesante es el de Irlanda, que invirtió 50 millones de euros en el sistema de

votación electrónico PowerVote desarrollado por la empresa Nedap, que se negó a entregar los códigos fuentes del programa alegando protección de copyright sobre éstos. El único arreglo que la empresa aceptó fue que un tercero imparcial auditara las urnas bajo cláusulas de confidencialidad. La auditoría no sólo es técnicamente casi imposible, sino que además está limitada jurídicamente por términos de copyright. La prohibición de auditar por términos de copyright no es un caso aislado. Lo mismo está ocurriendo hoy día con las urnas compradas por el Estado de Nueva Jersey.

Lo barato sale caro

Una frase repetida por los promotores del voto electrónico es que es más barato. En el proyecto de ley a nivel nacional, los legisladores del Frejuli no quieren abundar "en consideraciones de índole económica –que son conocidas por todos– en punto a los menores costos que significa la implementación de esta modalidad". Los diputados no ofrecen documentación alguna para sostener su afirmación.

Mientras que en los EE.UU. los promotores del sistema también recurrían a ese tipo de muletillas, los auditores independientes los pusieron a prueba. En el Estado de Maryland, entre 2002 y 2003, se compraron 19 mil máquinas de pantalla táctil a la firma Diebold. Para poder concretar la compra, el Estado tomó un crédito de 67 millones de dólares, 44 de los cuales fueron a las arcas de la empresa en concepto de compra y mantenimiento de las urnas. Antes de incorporar estos dispositivos, Maryland usaba un sistema de lector óptico. Según el informe de la organización **Save Our Votes** publicado en febrero de 2008, el cambio de tecnologías implicó un aumento promedio de 179% en el costo total por votante. En uno de los condados, el aumento fue de 866%. Por cierto, las máquinas de Diebold todavía no se terminaron de pagar y deben ser renovadas. El Estado de Maryland está considerando volver al sistema de lector óptico.

La Democracia privatizada

Muchas empresas proveedoras de urnas electrónicas están involucradas en el lobby por la modificación del sistema electoral y en el marketing sobre los beneficios del voto electrónico.

En el año 2003, la empresa española Indra promocionó sus servicios facilitando gratuitamente una prueba piloto para las elecciones municipales en Ushuaia. En aquel año, intendente y concejales fueron electos con voto electrónico, en la que aparece como la primera implementación de este tipo en el país. Llegadas las elecciones de 2007, Ushuaia se disponía a repetir la experiencia, pero antes debía llamar a licitación para comprar los equipos. Gracias a su gentileza de 2003, Indra era la que tenía mayores ventajas.

Los concejales de Ushuaia tuvieron el tino de exigir que la licitación contemplara una larga

nómina de recaudos de seguridad, entre ellos que las urnas emitieran un comprobante en papel. Ofendida por la exigencia de los concejales, y alegando que una elección de ese tipo dejaría de ser voto electrónico, Indra se retiró de la licitación. Ushuaia volvió a votar en papel.

Por supuesto, Indra es una empresa, así como lo son Nedap, Diebold o ES&S. Su misión es hacer negocios y ganar dinero para sus accionistas. El problema es que, en este caso, el negocio pone en riesgo al sistema electoral. La pregunta que surge tiene que ver con los riesgos de privatizarlo, a favor de una dudosa modernidad.

Holanda vuelve a usar papel y lápiz para votar

'We do not trust voting computers'

(No confiamos en computadoras de votación) se movilizó para asegurar que el sistema de votación holandés vuelva a ser confiable como era antes de que se incorporaran las computadoras de votación sin papel. Y esto es lo que han obtenido: El 27 de septiembre de 2007, la Comisión Asesora para el Proceso Electoral publicó el informe llamado 'Votar con confianza'. Inmediatamente, la Secretaría de Estado para el Interior anunció que la 'Regulación para la aprobación de las máquinas de votación de 1997' sería eliminada. El 1 de octubre de 2007, la Corte Distrital de Amsterdam retiró la certificación de las computadoras de votación Nedap, actualmente en uso en Holanda. Esta orden de la corte es el resultado de una campaña iniciada por 'We do not trust voting computers' en marzo de 2007. El 21 de octubre de ese mismo año, la regulación que aprobaba el uso de computadoras para votar fue efectivamente descartada.

El 16 de mayo de 2008, el Gobierno Holandés resolvió que las elecciones en Holanda serán realizadas usando sólo boletas en papel y lápices rojos. La propuesta para trabajar en el desarrollo de una nueva generación de computadoras de votación fue descartada completamente.

Fuente:
http://www.wijvertrouwenstemcomputersniet.nl/English

Exponen los errores de las urnas electrónicas de Ohio

Las máquinas no se pueden arreglar antes del 4 de noviembre, dice Brunner

Los electores norteamericanos seguirán votando con máquinas que pierden votos.

La empresa fabricante de las máquinas de votación que se usan en la mitad de los condados del Estado de Ohio en EEUU admitió que tienen errores de programación que hacen que se pierdan votos. "El problema no puede ser resuelto antes de las elecciones del 4 de noviembre, por lo que los ejecutivos de Premier Election Solutions (antes Diebold) y la Secretaria de Estado Jennifer Brunner están trabajando en una serie de guías para que los condados puedan detectar y evitar estos problemas" informó The Columbus Dispatch.

La Ex Diebold había especulado inicialmente con que el problema de la pérdida de votos se debía a un conflicto entre su propio sistema y el software anti-virus que ejecutan las máquinas. Pero posteriormente, en una carta enviada a Brunner, el presidente de Premier, David Byrd, admitió que la pérdida de votos se debe, en realidad, a un problema en el código fuente de sus programas y que no será resuelto antes de las próximas elecciones presidenciales en los EEUU.

Recordemos que meses atrás, Premier Election Solutions había dicho que el problema de pérdida de votos se debía a una incompatibilidad del sistema operativo usado con el antivirus que funciona en las urnas.

Fuente:
http://dispatch.com/live/content/local_news/stories/2008/08/21/voting_machines.html?sid=101
The Columbus Dispatch
Resumen en español en
http://www.vialibre.org.ar/2008/09/28/las-maquinas-de-votacion-no-se-arreglan-antes-de-4-de-noviembre/

Problemas de votación en varios estados de los EEUU

Un nuevo informe de la Oficina de Responsabilidad Gubernamental sobre el sistema de votación indica que la Comisión de Asistencia en Elecciones no ha notificado a los oficiales electorales de numerosos condados sobre las fallas en las máquinas de emisión de votos. En tanto, un nuevo estudio de las organizaciones Common Cause y Century Foundation encontró que por lo menos 10 estados importantes tienen significativos problemas en sus sistemas de votación que no fueron resueltos desde la última elección. Estos 10 estados, según Common Cause son: Colorado, Florida, Georgia, Michigan, Missouri, New Mexico, Ohio, Pennsylvania, Virginia y Wisconsin.

Los problemas detectados van desde un amplio margen de errores en las máquinas de votación, hasta fallas en el registro electrónico. "Encontramos muchos problemas donde la gente está siendo eliminada de las bases de votación porque sus nombres están mal registrados: como por ejemplo, que digan Alex en lugar de Alexander o que contengan iniciales de segundo nombre o no" indicó Susan Geenhalgd de Voter Action. "Estos son problemas que están siendo creados por restricciones del software que son errores y que en muchos casos están quitando a la gente la posibilidad de votar". Esto se está solucionando con el otorgamiento de boletas provisorias para los votantes con problemas en el registro.

Tova Wang, de Common Cause dijo que hay una "alta probabilidad de que con la cantidad de nuevos votantes que tenemos, haya una demanda enorme de estas boletas provisorias" y agregó que excepto en uno de esos 10 estados "los estados involucrados no están haciendo nada para asegurarse que haya de estas boletas provisorias a mano en suficiente cantidad para no quedarse sin ellas" agregó.

Fuente:
CNN.
http://www.cnn.com/2008/POLITICS/09/18/voting.problems/index.html?iref=werecommend
Adaptación al español: Fundación Vía libre

La culpa es de la estática

Al parecer, problemas de estática provocaron el misterioso sobrante de votos registrado en las primarias de septiembre en Washington. Los oficiales del Consejo electoral de Washington DC encontraron una explicación a los 1500 votos fantasma registrados en las primarias de Septiembre, en las que 326 personas asistieron a votar en el Centro Reeves. Cuando sus votos fueron sumados, sin embargo, aparecieron 1500 sufragios de la nada, que según las explicaciones publicadas esta semana en la prensa, se debieron a una descarga de estática. "Una de las posibles causas podría ser una descarga de electricidad estática" dijo Errol Arthur, miembro del Consejo Electoral de Washington DC, lo que provocó reacciones que van desde la risa hasta la preocupación por parte de los votantes y demás miembros del consejo. El problema central es que esos mismos equipos que dibujaron 1500 votos fantasma en las primarias de septiembre serán utilizados en las presidenciales del próximo 4 de noviembre en el mismo condado.

Fuente:
http://www.news8.net/news/stories/1008/558138.html
Adaptación al español en
http://www.vialibre.org.ar/2008/10/03/la-culpa-es-de-la-estatica/

Jueza prohíbe la publicación de estudio de seguridad sobre urnas electrónicas

La jueza norteamericana Linda Feinberg solicitó a un grupo de investigadores de seguridad liderado por Andrew Appel que analizara la seguridad de las urnas electrónicas Sequoia AVC Advantage. El estudio fue encomendado como parte de un proceso que pide sacar de circulación estas urnas, que serán usadas en muchos precintos en las próximas elecciones presidenciales de los EEUU. Tres semanas luego de entregado el informe, la jueza prohibió la publicación del estudio.

El estado de New Jersey utiliza mayoritariamente este modelo de computadoras de Registro Electrónico Directo (RED) de votos, pero ninguna de las urnas puede ser auditada: las urnas tampoco dejan comprobante en papel que pueda servir para verificar si la máquina está contando los votos como realmente se emiten. El 24 de septiembre, la Juez Feinberg ordenó a los investigadores que no publiquen el informe que les había solicitado. Esta investigación es parte del juicio iniciado por la Clínica de Litigación Constitucional Rutgers, buscando el decomiso de todas las computadoras de votación de New jersey. Esto se debe a que no hay forma de saber si las máquinas cumplen o no con los principios constitucionales y con la ley estatutaria de contar los votos como debe.

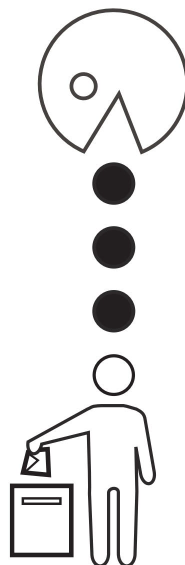
El conflicto sobre la publicación o no del informe ya ha sido discutido en la Corte, ya que se trata de que el público y los legisladores sepan realmente los hechos básicos sobre la confianza que pueden tener, o no, en el proceso electoral. Los mismos legisladores han solicitado acceso al informe, pero la Corte lo ha denegado. Incluso, el Gobernador y los Secretarios de Estado tienen negado el acceso al informe.

La firma Sequoia interpuso un recurso de protección alegando que el código fuente de sus programas incluye secretos

industriales que deben ser preservados. Así, el 24 de septiembre pasado, la Juez Feinberg prohibió la publicación del informe y censuró a los investigadores la posibilidad de hablar al respecto.

Fuente:
http://www.freedom-to-tinker.com/blog/appel/judge-suppresses-report-voting-machine-security

anexos



Manifesto dos Professores e Cientistas*

ALERTA CONTRA A INSEGURANÇA DO SISTEMA ELEITORAL INFORMATIZADO

SOMOS FAVORÁVEIS AO USO DA INFORMÁTICA NO SISTEMA ELEITORAL, MAS NÃO À CUSTA DA TRANSPARÊNCIA DO PROCESSO E SEM POSSIBILIDADE DE CONFERÊNCIA DOS RESULTADOS.

Cidadão brasileiro,

Nosso regime democrático está seriamente ameaçado por um projeto de lei em tramitação no Congresso Nacional, o Projeto do Voto Virtual, PL 1503/03. Este projeto, sob a máscara da modernidade, acaba com as alternativas de auditoria eficiente do nosso Sistema Eleitoral Informatizado, pois: (1) elimina o registro impresso do voto conferido pelo eleitor, substituindo-o por um "voto virtual cego", cujo conteúdo o eleitor não tem como verificar; (2) revoga a obrigatoriedade da Justiça Eleitoral efetuar uma auditoria aberta no seu sistema informatizado antes da publicação dos resultados finais; (3) permite que o Sistema Eleitoral Informatizado contenha programas de computador fechados, ou seja, secretos.

O Projeto de Lei do Voto Virtual nasceu por sugestão de ministros do Supremo Tribunal Federal e do Tribunal Superior Eleitoral (TSE), ao Senador Eduardo Azeredo, e sua tramitação tem sido célere, empurrado pela

interferência direta desses ministros sobre os legisladores, como declarado por estes durante a votação no Senado.

As Comissões de Constituição e Justiça das duas casas legislativas analisaram a juridicidade do projeto mas, apesar dos constantes alertas de membros da comunidade acadêmica para seus riscos sem rigorosos procedimentos de auditoria e controle, nenhuma audiência pública com especialistas em Informática e Segurança de Dados foi realizada.

Essa lei, se aprovada, trará como resultado a instituição de um sistema eleitoral no qual não se poderá exercer uma auditoria externa eficaz, pondo em xeque até os fundamentos do projeto democrático brasileiro. Aceitando essa interferência e implantando um sistema eleitoral obscuro, corremos o risco de virmos a ser governados por uma dinastia, com os controladores do sistema eleitoral podendo eleger seus sucessores, mesmo sem ter os votos necessários.

A nação, anestesiada pela propaganda oficial, lamentavelmente desconhece o perigo que corre. Os meios de comunicação, com honrosas exceções, omitem-se inexplicavelmente, como se o assunto não fosse merecedor de nossa preocupação.

A finalidade deste alerta é a denúncia da falta de confiabilidade de um sistema eleitoral informatizado que: utiliza programas de computador fechados, baseia-se em urnas eletrônicas sem materialização do voto, não propicia meios eficazes de fiscalização e auditoria pelos partidos políticos, e identifica o eleitor por meio da digitação do número de seu título eleitoral na mesma máquina em que vota. Assim, o princípio da inviolabilidade do voto, essencial numa democracia, será respeitado apenas na medida em que os controladores do sistema eleitoral o permitirem, transformando-se o voto secreto em mera concessão.

Uma verdadeira caixa-preta a desafiar nossa fé, este sistema é inauditável, inconfiável e suscetível de fraudes informatizadas de difícil detecção. Como está, ele seria rejeitado na mais simples bateria de testes de confiabilidade de sistemas pois, em Informática, "Sistema sem fiscalização é sistema inseguro". Muitas das fraudes que ocorriam quando o voto era manual, foram eliminadas, mas o cidadão brasileiro não foi alertado de que, com a informatização, introduziu-se a possibilidade de fraudes eletrônicas mais sofisticadas, mais amplas e mais difíceis de serem descobertas.

Enquanto os países adiantados caminham no sentido de exigir que sistemas eleitorais informatizados possuam o registro material do voto, procedam auditoria automática do sistema e só utilizem programas de computador abertos, com esse Projeto de Lei do Voto Virtual, o Brasil vai na contramão da história.

De que adianta rapidez na publicação dos resultados, se não respeitarmos o direito do cidadão de verificar que seu voto foi corretamente computado? Segurança de dados é assunto técnico especializado e assusta-nos a falta de seriedade com que nossa votação eletrônica tem sido tratada, nos três Poderes, por leigos na matéria. Os rituais promovidos pelo TSE, como a apresentação dos programas, a carga das urnas e os testes de simulação são apenas espetáculos formais, de pouca significância em relação à eficiência da fiscalização.

Surpreende-nos, sem desmerecer suas competências na área jurídica, que autoridades respeitáveis da Justiça Eleitoral possam anunciar, com toda a convicção, que o sistema eleitoral informatizado é "100% seguro" e "orgulho da engenharia nacional", externando inverdades em áreas que não dominam, alheias ao seu campo de conhecimento específico.

Para o eleitor, a urna é 100% insegura, pois pode ser programada para "eleger" desde vereadores até o próprio presidente. O único e mais simples antídoto para esta insegurança é a participação individual do eleitor na fiscalização do registro do seu próprio voto, pois ele é o único capaz de fazer isto adequadamente.

O TSE sempre evitou debater tecnicamente a segurança da urna, ignorando todas as objeções técnicas em contrário. Nenhum estudo isento e independente foi feito até hoje sobre a alegada confiabilidade da urna sem o voto impresso. O estudo de um grupo da Unicamp (pago pelo TSE), parcial e pleno de ressalvas, recomendou vários procedimentos como condição para garantir o nível de segurança necessário ao sistema. Essas ressalvas, infelizmente, foram omitidas na propaganda sobre as maravilhas da urna.

A confiabilidade de sistemas informatizados reside nas pessoas e nas práticas seguras. Palavras mágicas como assinatura digital, criptografia assimétrica, embaralhamento pseudo-aleatório e outras panacéias de nada valem se não forem acompanhadas de rigorosos procedimentos de verificação, fiscalização e auditoria externas. Se esta urna algum dia cair sob o controle de pessoas desonestas, elas poderão eleger quem desejarem. De modo algum podemos confiar apenas nas pesquisas eleitorais como modo de validar os resultados das urnas eletrônicas, especialmente se as diferenças entre os candidatos forem pequenas.

Nenhum sistema informatizado é imune à fraude, especialmente a ataques internos, como sucedeu em julho de 2000 com o Painel Eletrônico do Senado, fato que levou à renúncia de dois senadores. A única proteção possível é um projeto cuidadoso que atenda aos requisitos de segurança, e à possibilidade de auditorias dos programas, dos procedimentos e dos resultados.

Basta de obscurantismo no sistema eleitoral. Enfatizamos a necessidade de serem realizados debates técnicos públicos e independentes sobre a segurança do sistema e de seus defeitos serem corrigidos, antes da aprovação de leis que comprometam a transparência do processo.

A democracia brasileira exige respeito ao Princípio da Transparência e ao Princípio da Tripartição de Poderes no processo eleitoral.

Instamos todos os eleitores preocupados com a confiabilidade de nosso sistema eleitoral a transmitirem suas preocupações, por todos os meios possíveis, a seus representantes no Congresso e aos meios de comunicação. Brasil, setembro de 2003

Signatários:

Walter Del Picchia
Professor Titular da Escola Politécnica da Universidade de São Paulo - USP

Jorge Stolfi
Professor Titular do Instituto de Computação da Universidade Estadual de Campinas - UNICAMP

Michael Stanton
Professor Titular do Depto. de Ciência da Computação da Universidade Federal Fluminense - UFF

Routo Terada
Professor Titular do Depto. de Ciências da Computação do Instituto de Matemática e Estatística da Universidade de São Paulo - USP

Edison Bittencourt
Professor Titular da Faculdade de Engenharia Química da Universidade de Campinas - UNICAMP

Pedro Dourado Rezende
Professor do Depto. de Ciência da Computação da Universidade de Brasília - UNB - Representante da Sociedade Civil no Comitê Gestor da Infra-estrutura de Chaves Públicas ICP-Brasil

Paulo Mora de Freitas
Chefe do serviço de Informática do Laboratório Leprince-Ringuet da Ecole Polytechnique, Palaiseau, França

José Ricardo Figueiredo
Professor Dr. do Departamento de Energia da Faculdade de Engenharia Mecânica da Universidade de Campinas - UNICAMP

Notas

* Original en Portugués. Documento disponible en línea en http://www.votoseguro.com/alertaprofessores/ (última consulta 28/09/08).
NdE: Este documento fue publicado por los principales profesores e investigadores en Seguridad Informática de Brasil como alerta frente a los cambios introducidos por el Tribunal Superior Electoral en Brasil en septiembre de 2003.

Ordenanza derogatoria del Voto Electrónico en San Antonio Oeste *

VISTO: La Ordenanza 2454, en la que se adhiere en todos sus términos a la Ley Provincial N°4082/06 del sistema de voto electrónico y

CONSIDERANDO:

- Que la implementación del voto electrónico en las últimas elecciones municipales, en el 50% de las mesas electorales del Balneario Las Grutas, no dieron el resultado esperado, muy por el contrario generaron demoras, trastornos e incertidumbre durante el acto eleccionario.
- Que los argumentos para la implementación del voto electrónico eran entre otros, la celeridad y facilidad en la emisión del voto. Pero que en la práctica nada de eso sucedió ya que en la carga de los padrones a las máquinas por parte de ALTEC, faltaron datos de personas que sí figuraban en el soporte de papel. Dando origen a la realización de un acta con los representantes de la Junta Electoral Municipal atribuyendo las fallas a "un error de formato" del sistema.
- Que un porcentaje muy alto de votantes pertenecientes a las mesas 1 y 2 femeninas, que figuraban en el padrón manual pero que no aparecían en el padrón digital y la máquina les impedía votar, debieron ser autorizadas a emitir su voto en las otras 2 mesas tradicionales. Generando demoras y trabajo extra ya que debían ser asentados los datos del votante manualmente en el padrón por parte de las autoridades de mesa.
- Que sobre el final del acto eleccionario, cuando las autoridades de la mesa 2 masculina pretendieron retirar

la memoria extraíble para guardarla en el sobre y apretar el botón para que tire el escrutinio, existió una falla técnica que borró la memoria y obligó al recuento en forma manual de los tickets que quedan en el interior de la urna electrónica. Hecho que pudo realizarse a altas horas de la noche, generando nerviosismo y dudas sobre el destino de los votos emitidos.

- Que sólo votó el 40% de los votantes que se encontraban en el padrón de las urnas electrónicas, mientras que en las mesas de voto tradicional votó el 70% de los empadronados. Demostrando en la población una manifiesta desconfianza y desconocimiento del sistema, lo que generó la escasa participación en un acto imprescindible de la democracia. Generando un sentimiento de discriminación en aquellos que caprichosamente formaban parte del sistema digital.
- Que por todo lo enunciado precedentemente, el sistema hoy no da garantías de mejorar la emisión tradicional del sufragio.

POR ELLO:

EL CONCEJO DELIBERANTE DE SAN ANTONIO OESTE Sanciona con fuerza de ORDENANZA

- ARTICULO 1: Deróguese la Ordenanza N°2454/06 que adhire en todos sus términos a la Ley N° 4082/06 de creación del Sistema de Voto electrónico.

- ARTICULO 2: DE FORMA

INFORME: VOTO ELECTRONICO ELECCIONES MUNICIPALES DEL 16 DE DICIEMBRE DE 2007, SAN ANTONIO OESTE.

En referencia a que se nos ha pedido que nos expresemos en voluntad de reflejar nuestra opinión y experiencia con la utilización de la modalidad del voto electrónico es que mencionamos lo siguiente:

La informática como parte de la tecnología es una herramienta muy eficiente para resolver una infinidad de problemas que hacen a la vida cotidiana de toda sociedad. Sin embargo creer que tenemos dominio, poder o control sobre este tipo de tecnología especifica es lo más erróneo que podemos pensar.

- Esta característica de continuo dinamismo hace de la informática una herramienta muy sofisticada y compleja como para especular que gozamos cierto control sobre las situaciones que se pueden presentar.
- Ustedes ni nosotros jamás conseguiremos afirmar con esta tecnología que la inviolabilidad del secreto de voto

de cada ciudadano está a resguardo de su derecho supremo, sino que únicamente conseguiremos confiar que las personas a cargo de estas tecnologías hacen lo correcto.

- Así como lo vemos, el hombre en su naturaleza únicamente puede sentirse seguro, confiado de todo aquello que éel cree que conoce.
- Atribuirnos el poder y la voluntad de que por que algunos puedan creerse dueños de estas tecnologías, el resto de la sociedad deba confiar a ciegas en algo de lo que nunca en su más criteriosa voluntad va a ser capaz de confiar es muy miserable de nuestra parte y responsabilidad.
- Hoy con más experiencia y responsabilidad que la que tuvimos cuando asumimos la tarea de instrumentar la modalidad del voto electrónico estamos convencidos que no volveríamos a repetir el modo.
- ¿A quién responsabilizar por todo los inconvenientes y dificultades que pasaron, antes, durante y después del acto eleccionario? Decir que la ciencia fallo sería muy fácil. Decir que la sociedad nunca terminó de aceptar el compromiso hacia aquello que se le había facilitado sería muy cómodo también. Decir que unos pocos técnicos de una empresa informática fallaron sería aún más fácil.
- Que todos aquellos que custodiamos el sentir de la Ley Electoral reconozcamos que hemos fallado es más difícil. Nosotros como integrantes de la Junta Electoral Municipal de San Antonio Oeste nos vemos en la obligación de reconocer que nos hemos equivocado al tomar ciertas decisiones en función de anteponer los intereses de agrupaciones políticas, gobierno y entidades privadas sobre los intereses y sentimientos de nuestros vecinos. Nunca encontraremos palabras para explicarles a nuestros vecinos que algo tan simple como que un ciudadano que está habilitado como elector en una mesa lo tenga que hacer en otra mesa por que ha ocurrido una falla en la urna electrónica.
- Que al momento del escrutinio la urna electrónica pierda los datos o no pueda informar un resultado por que ha ocurrido una falla en algo que está realizado con la finalidad de dar seguridad. Muchos problemas y pocas respuestas que puedan compensar el sentimiento de malestar y angustia de nuestros vecinos.

Notas

* NdE.: Esta ordenanza fue aprobada en el mes de Julio de 2008 en el Concejo Deliberante de la Ciudad de San Antonio Oeste / Las Grutas para derogar la Ordenanza 2454 que autorizó el uso de urnas electrónicas en las elecciones municipales del 16 de diciembre de 2007.